

**BURSOR & FISHER, P.A.**

Joshua R. Wilner (State Bar No. 353949)  
1990 North California Blvd., 9th Floor  
Walnut Creek, CA 94596  
Telephone: (925) 300-4455  
Facsimile: (925) 407-2700  
E-mail: ehorne@bursor.com  
jwilner@bursor.com

**BURSOR & FISHER, P.A.**

Philip L. Fraietta (State Bar No. 354768)  
1330 Avenue of the Americas, 32nd Floor  
New York, NY 10019  
Telephone: (646) 837-7150  
Facsimile: (212) 989-9163  
E-mail: pfraietta@bursor.com

*Attorneys for Plaintiff*

[additional counsel on signature page]

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

TREVOR HARRIS, individually and on  
behalf of all other persons similarly situated,

Plaintiff,

v.

IHEARTMEDIA, INC.,

Defendant.

Case No.

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

**TABLE OF CONTENTS**

|   | <b>PAGE</b> |
|---|-------------|
| NATURE OF THE ACTION .....  | 1           |
| THE PARTIES .....   | 2           |
| JURISDICTION AND VENUE .....  | 2           |
| FACTUAL ALLEGATIONS .....   | 3           |
| I. THE CALIFORNIA INVASION OF PRIVACY ACT PROTECTS CALIFORNIANS’ RIGHT TO CONTROL THE DISSEMINATION OF THEIR ELECTRONIC COMMUNICATIONS .....                    | 3           |
| II. DEFENDANT VIOLATES THE CALIFORNIA INVASION OF PRIVACY ACT.....  | 5           |
| A. The Mechanics And Privacy Implications Of IP Addresses .....   | 6           |
| 1. Differentiating Between A Public Versus Private IP Address .....   | 6           |
| 2. The Privacy Implications Of Public IP Addresses .....  | 9           |
| B. The Trackers Are “Pen Registers” That Defendant And The Third Parties Use To De-Anonymize And Identify Users And Sell Their Information To Advertisers ..... | 12          |
| 1. The ADNXS Tracker And The Data Broker Partners It Cookie Syncs With.....   | 13          |
| (i) Experian/Tapad.....   | 16          |
| (ii) Lotame .....   | 18          |
| (iii) TransUnion/Neuster .....  | 21          |
| 2. The TripleLift Tracker And The Data Broker Partners It Cookie Syncs With.....  | 25          |
| (i) Lotame .....  | 27          |
| 3. The OpenX Tracker And The Data Broker Partners It Cookie Syncs With.....   | 28          |
| (i) Microsoft, TripleLift, Experian, And Lotame .....   | 31          |
| (ii) LiveRamp .....   | 31          |
| III. DEFENDANT’S CONDUCT CONSTITUTES AN INVASION OF PLAINTIFF’S AND CLASS MEMBERS’ PRIVACY.....   | 34          |
| A. Data Brokers And Real-Time Bidding: The Information Economy .....  | 35          |
| 1. Data Brokers .....   | 35          |

1                   2.     Real-Time Bidding .....39

2                   3.     Cookie Syncing .....44

3                B.     Defendant Uses The ADNXS Tracker For Targeted Advertising,  
                  Identity Resolution, And Data Monetization.....47

4                C.     Defendant Uses the TripleLift Tracker For Targeted Advertising  
                  Identity Resolution, And Data Monetization.....49

5                D.     Defendant Uses The OpenX Tracker For Targeted Advertising,  
                  Identity Resolution, And Data Monetization.....51

6                D.     Defendant Uses The OpenX Tracker For Targeted Advertising,  
                  Identity Resolution, And Data Monetization.....51

7   IV.    PLAINTIFF’S EXPERIENCE .....53

8   V.    DEFENDANT IS SUBJECT TO JURISDICTION IN CALIFORNIA.....55

9   CLASS ALLEGATIONS .....58

10 CAUSES OF ACTION.....60

11 PRAYER FOR RELIEF .....62

12 JURY DEMAND.....62

1 Plaintiff Trevor Harris (“Plaintiff”), individually and on behalf of all others similarly situated,  
2 by and through his attorneys, makes the following allegations pursuant to the investigation of his  
3 counsel and based upon information and belief, except as to allegations specifically pertaining to  
4 himself and his counsel, which are based on personal knowledge.

5 **NATURE OF THE ACTION**

6 1. Defendant iHeartMedia, Inc. (“Defendant” or “iHeart”) owns and operates a website,  
7 iheart.com (the “Website”), which is a digital platform with broadcast, podcast, radio, and music  
8 streaming.

9 2. When users visit the Website, Defendant causes at least three Trackers—the ADNXS  
10 Tracker, the TripleLift Tracker, and the OpenX Tracker (collectively, the “Trackers”)—to be  
11 installed on Website visitors’ internet browsers. The Trackers are operated by separate and distinct  
12 third parties: Microsoft, TripleLift, and OpenX (the “Third Parties”). Through their respective  
13 Trackers, each of the Third Parties collect Website users’ internet protocol (“IP”) addresses and other  
14 device identifier information such as device type, browser type, and unique and persistent identifiers  
15 (the “Device Metadata”).

16 3. Defendant then uses the data collected by the Trackers, and in conjunction with the  
17 Third Parties operating them, for targeted marketing and advertising that enable Defendant to  
18 monetize its Website. That is, Defendant and the Third Parties benefit from the Third Parties’  
19 unconsented-to collection of Plaintiff’s and Class Members’ personal information.

20 4. Because the Trackers capture Website visitors’ “routing, addressing, or signaling  
21 information,” the Trackers constitute a “pen register” under Section 638.50(b) of the California  
22 Invasion of Privacy Act (“CIPA”).

23 5. By installing and using the Trackers without Plaintiff’s prior consent and without a  
24 court order, Defendant violated CIPA § 638.51(a).

25 6. The conduct here is more invasive because of the entities operating the Trackers and  
26 collecting Plaintiff’s and Class Members’ IP Addresses and Device Metadata. OpenX is a data  
27 broker. Microsoft and TripleLift link the information they collect about Website users with other  
28

1 data brokers whose trackers Defendant also installs on Website users' browsers. These trackers add  
2 the IP addresses and Device Metadata of Website users to comprehensive user profiles and use that  
3 information to track Plaintiff and Class Members across the Internet. Those data profiles are then  
4 provided to advertisers for more targeted and tailored advertising based on a broad universe of  
5 information. The Third Parties also facilitate that targeted advertising by using IP addresses and  
6 Device Metadata to sell Defendant's user inventory to advertisers and allow advertisers to target  
7 specific users or groups of users with specific advertisements based on that information, including  
8 Website users' location. All of this enriches Defendant, who is able to monetize its Website as the  
9 beneficiary of that advertising revenue. Indeed, Defendant increases the value of its user base to  
10 prospective advertisers by allowing OpenX, and other data brokers to connect IP addresses and  
11 Device Metadata to broader profiles of other personal information.

12 7. Plaintiff brings this action to prevent Defendant from further violating the privacy  
13 rights of California residents, and to recover statutory damages for Defendant's violation of CIPA  
14 § 638.51.

### 15 **THE PARTIES**

16 8. Plaintiff Trevor Harris resides in Salinas, California and has an intent to remain there,  
17 and is therefore a citizen of California. Plaintiff Harris was in California when he visited the Website.

18 9. Defendant iHeartMedia, Inc. is a Texas corporation with its principal place of  
19 business in San Antonio, Texas.

### 20 **JURISDICTION AND VENUE**

21 10. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C.  
22 § 1332(d)(2)(a) because this case is a class action where the aggregate claims of all members of the  
23 proposed class are in excess of \$5,000,000.00 exclusive of interest and costs, there are over 100  
24 members of the putative class, and at least one class member is a citizen of a different state than  
25 Defendant.

26 11. This Court has jurisdiction over Defendant for the reasons set forth below. *See*  
27 Factual Allegations § V, *infra*.

12. Venue is proper pursuant to 28 U.S.C. § 1391(b) because a substantial portion of the events giving rise to this action occurred in this District.

### **FACTUAL ALLEGATIONS**

#### **I. THE CALIFORNIA INVASION OF PRIVACY ACT PROTECTS CALIFORNIANS' RIGHT TO CONTROL THE DISSEMINATION OF THEIR ELECTRONIC COMMUNICATIONS**

13. The California Legislature enacted CIPA to protect certain privacy rights of California citizens. The California Legislature expressly recognized that “the development of new devices and techniques for the purpose of eavesdropping upon private communications ... has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.” Cal. Penal Code § 630.

14. As the California Supreme Court has held in explaining the legislative purpose behind CIPA:

While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its *simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or mechanical device*.

As one commentator has noted, such secret monitoring denies the speaker an important aspect of privacy of communication—*the right to control the nature and extent of the firsthand dissemination of his statements*.

*Ribas v. Clark*, 38 Cal. 3d 355, 360-61 (1985) (emphasis added; internal citations omitted).

15. As relevant here, CIPA § 638.51(a) proscribes any “person” from “install[ing] or us[ing] a pen register or a trap and trace device without first obtaining a court order.”

16. A “pen register” is a “a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication.” Cal. Penal Code § 638.50(b).

17. A “trap and trace device” is a “a device or process that captures the incoming electronic or other impulses that identify the originating number or other dialing, routing, addressing,

1 or signaling information reasonably likely to identify the source of a wire or electronic  
2 communication, but not the contents of a communication.” Cal. Penal Code § 638.50(b).

3 18. In plain English, a “pen register” is a “device or process” that records *outgoing*  
4 information, while a “trap and trace device” is a “device or process” that records *incoming*  
5 information.

6 19. Historically, law enforcement used “pen registers” to record the numbers of outgoing  
7 calls from a particular telephone line, while law enforcement used “trap and trace devices” to record  
8 the numbers of incoming calls to that particular telephone line. As technology has advanced,  
9 however, courts have expanded the application of these surveillance devices to the Internet.

10 20. For example, if a user sends an email, a “pen register” might record the email address  
11 it was sent from because this is the user’s *outgoing* information. On the other hand, if that same user  
12 receives an email, a “trap and trace device” might record the email address it was sent from because  
13 this is *incoming* information that is being sent to that same user.

14 21. Although CIPA was enacted before the dawn of the Internet, “the California Supreme  
15 Court regularly reads statutes to apply to new technologies where such a reading would not conflict  
16 with the statutory scheme.” *In re Google Inc.* 2013 WL 5423918, at \*21 (N.D. Cal. Sep. 26, 2013).  
17 For this reason, courts have regularly applied the CIPA to Internet tracking technologies such as  
18 those here. *See, e.g., Shah v. Fandom, Inc.*, 754 F. Supp. 3d 924, 930 (N.D. Cal. 2024) (finding  
19 trackers similar to those at issue here were “pen registers” and noting “California courts do not read  
20 California statutes as limiting themselves to the traditional technologies or models in place at the  
21 time the statutes were enacted”); *Mirmalek v. Los Angeles Times Communications LLC*, 2024 WL  
22 5102709, at \*3-4 (N.D. Cal. Dec. 12, 2024) (same); *Moody v. C2 Educ. Sys. Inc.* 742F. Supp. 3d  
23 1072, 1076 (C.D. Cal. 2024) (“Plaintiff’s allegations that the TikTok Software is embedded in the  
24 Website and collects information from visitors plausibly fall within the scope of §§ 638.50 and  
25 638.51.”); *Greenley v. Kochava, Inc.*, 684 F. Supp. 3d 1024, 1050 (S.D. Cal. 2023) (referencing  
26 CIPA’s “expansive language” when finding software was a “pen register”); *Javier v. Assurance IQ*,  
27  
28

1 *LLC*, 2022 WL 1744107, at \*1 (9th Cir. May 31, 2022) (“Though written in terms of wiretapping,  
2 [CIPA] Section 631(a) applies to Internet communications.”).

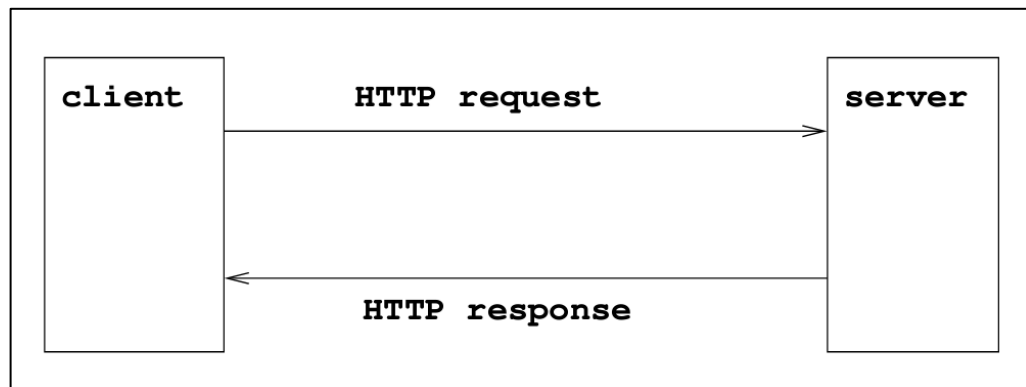
3 22. This accords with the fact that, “when faced with two possible interpretations of  
4 CIPA, the California Supreme Court has construed CIPA in accordance with the interpretation that  
5 provides the greatest privacy protection.” *Matera v. Google Inc.*, 2016 WL 8200619, at \*19 (N.D.  
6 Cal. Aug. 12, 2016).

7 23. Individuals may bring an action against the violator of any provision of CIPA—  
8 including CIPA § 638.51—for \$5,000 per violation. Cal. Penal Code § 637.2(a)(1).

## 9 **II. DEFENDANT VIOLATES THE CALIFORNIA INVASION OF PRIVACY ACT**

10 24. To make Defendant’s Website load on a user’s internet browser, the browser sends  
11 an “HTTP request” or “GET” request to Defendant’s server where the relevant Website data is  
12 stored. In response to the request, Defendant’s server sends an “HTTP response” back to the  
13 browser with a set of instructions. A general diagram of this process is pictured at Figure 1, which  
14 explains how Defendant’s Website transmits instructions back to users’ browsers in response to  
15 HTTP requests.  
16

17 **Figure 1:**



18 25. The server’s instructions include how to properly display the Website—*e.g.*, what  
19 images to load, what text should appear, or what music should play.  
20

21 26. In addition, the server’s instructions cause the Trackers to be installed on a user’s  
22 browser. The Trackers then cause the browser to send identifying information—including the  
23  
24  
25  
26  
27  
28



1 user's IP address and Device Metadata—to Microsoft, TripleLift, and OpenX. These Third Parties,  
 2 through their Trackers, also set a cookie on Website users' browsers, which sends a unique  
 3 identifier to these Third Parties that allows them to track users on the Website over multiple visits  
 4 and across the Internet.

5 27. Plaintiff and Class Members did not provide their prior consent to Defendant to  
 6 install the Trackers on their browsers or use the Trackers. Nor did Defendant obtain a court order  
 7 before installing or using the Trackers.

8 **A. The Mechanics And Privacy Implications Of IP Addresses**

9 28. An IP address is a unique identifier for a device, which is expressed as four sets of  
 10 numbers separated by periods (*e.g.*, 192.168.123.132). The traditional format of IP addresses is  
 11 called IPv4, and it has a finite amount of combinations and thus is limited to approximately 4.3  
 12 billion addresses. Because this proved to be insufficient as the Internet grew, IPv6 was introduced.  
 13 IPv6 offers a vastly larger address space with 340 undecillion possible addresses. While IPv6  
 14 adoption has been increasing, many networks still rely on IPv4.<sup>1</sup>

15 29. Much like a telephone number, an IP address guides or routes an intentional  
 16 communication signal (*i.e.*, a data packet) from one device to another. An IP address is essential  
 17 for identifying a device on the internet or within a local network, facilitating smooth  
 18 communication between devices.

19 *1. Differentiating Between A Public Versus Private IP Address*

20 30. A public IP address is accessible from anywhere on the internet; it is assigned by an  
 21 Internet Service Provider ("ISP") and it is unique globally. Public IP addresses are required for  
 22 devices that need direct internet access.

23 31. While public IP addresses are unique, they are not necessarily "public" in the sense  
 24 that they are freely accessible. If an individual is not actively sending data packets out, the public IP  
 25 address remains private and is not broadcast to the wider internet.

26  
 27 <sup>1</sup> See, *e.g.*, *What is the Internet Protocol*, CLOUDFLARE, <https://www.cloudflare.com/learning/network-layer/internet-protocol/>; Stefano Gridelli, *What is an RFC1918 Address?*, NETBEEZ (Jan. 22, 2020), <https://netbeez.net/blog/rfc1918/>.  
 28

1           32. Public IP addresses can be used to determine the approximate physical location of a  
2 device. For example, services like iplocation.io, use databases that map IP addresses to geographic  
3 areas—often providing information about the country, city, approximate latitude and longitude  
4 coordinates, or even the internet service provider associated with the public IP. This geolocation  
5 capability is leveraged by online advertising and user identification services.

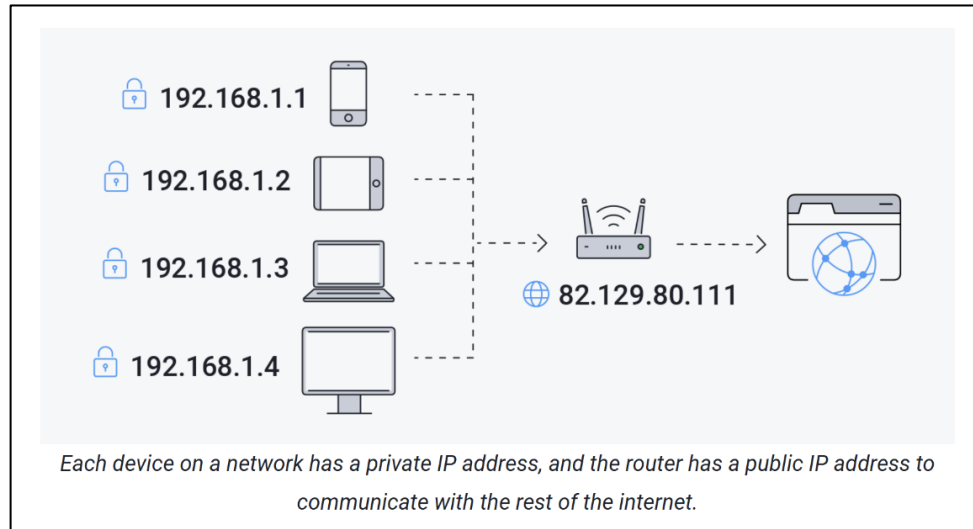
6           33. A private IP address is used within an internal network and is not routable on the  
7 public internet. The Internet Assigned Numbers Authority (“IANA”) reserves specific ranges of  
8 numbers to be exclusively used for private IP addresses (*e.g.*, 172.16.0.0 through 172.31.255.255).  
9 Thus, private IP addresses can be used repeatedly across different networks because they are isolated  
10 from the global internet. For example, a home network in New York and an office network in Tokyo  
11 can both use the same private IP address (*e.g.*, 192.168.1.1) for their routers without conflict.

12           34. The distinction between a public and private IP address is fundamental to the  
13 architecture of modern networks. Public IP addresses facilitate global communication, while private  
14 IP addresses conserve the finite amount of combinations to make an IP address through local network  
15 communication. And crucially, a private IP address does not divulge a user’s geolocation, whereas  
16 a public IP address does and is thus extensively used in advertising.

17           35. An analogy is useful. A public IP address is like the number for a landline telephone  
18 for a household. A private IP address is like each handset that is connected to that landline number  
19 (*e.g.*, “Handset #1,” “Handset #2”). A lot can be gleaned from knowing the phone number who is  
20 making the call, while knowing Handset #1 versus Handset #2 is making a call provides additional  
21 information.

22           36. The same is true of IP addresses. The public IP address divulges the approximate  
23 location of the user that is connecting to the Internet and the router directing those communications  
24 (presumably the user’s house or workplace), and it is the means through which the user actually  
25 communicates with the website and the Internet at large. The private IP address then distinguishes  
26 between the devices accessing the same public IP address.<sup>2</sup>

27 <sup>2</sup> While the Trackers do not collect private IP addresses, as discussed below, the Trackers also collect  
28 Device Metadata, which distinguishes between devices accessing the same public IP address. So,

**Figure 2:**

37. Thus, the differences between public and private IP addresses are as follows:<sup>3</sup>

**Figure 3:**

| Category      | Private IP address  | Public IP address   |
|---------------|---|---|
| Scope         | The private IP address only has a local scope in your own network.  | The public IP address's scope is global.  |
| Communication | It is used so devices within a network can communicate with each other.   | It allows access to the internet and is used for communication outside of your own network. |
| Uniqueness    | It's an address from a smaller range that's used by other devices in other local networks.                                | It's a unique address that's not used by other devices on the internet.                     |
| Provider      | The router assigns a private IP address to a specific device on the local network.  | The internet service provider assigns the public IP address.                                |
| Range         | Private IP address ranges:<br>10.0.0.0 – 10.255.255.255,<br>172.16.0.0 – 172.31.255.255,<br>192.168.0.0 – 192.168.255.255 | Any IP address that isn't within a private IP address range.                                |

38. A public IP address is therefore “routing, addressing, or signaling information.”

by installing the Trackers on Website users’ browsers, Defendant allows third parties to collect information that is analogous to a telephone number (the public IP address) and the specific handset that is making the call (the Device Metadata).

<sup>3</sup> WHAT’S THE DIFFERENCE BETWEEN A PUBLIC AND PRIVATE IP ADDRESS?, AVIRA (Jan. 31, 2024), <https://www.avira.com/en/blog/public-vs-private-ip-address>.

39. A public IP address is “addressing” information because it determines the general geographic coordinates of the user who is accessing a website.

40. A public IP address is “routing” or “signaling” information because it is sending or directing the user’s communication from the router in their home or work to the website they are communicating with, and ensuring that “emails, websites, streaming content, and other data reaches you correctly.”<sup>4</sup>

## 2. *The Privacy Implications Of Public IP Addresses*

41. Through a public IP address, a device’s state, city, zip code, and approximate latitude and longitude can be determined. Thus, knowing a user’s public IP address—and therefore geographical location—“provide[s] a level of specificity previously unfound in marketing.”<sup>5</sup>

42. A public IP address allows advertisers to (i) “[t]arget [customers by] countries, cities, neighborhoods, and ... postal code”<sup>6</sup> and (ii) “to target specific households, businesses[,] and even individuals with ads that are relevant to their interests.”<sup>7</sup> Indeed, “IP targeting is one of the most targeted marketing techniques [companies] can employ to spread the word about [a] product or service”<sup>8</sup> because “[c]ompanies can use an IP address ... to personally identify individuals.”<sup>9</sup>

43. In fact, a public IP address is a common identifier used for “geomarketing,” which is “the practice of using location data to identify and serve marketing messages to a highly-targeted audience. Essentially, geomarketing allows [websites] to better serve [their] audience by giving [them] an inside look into where they are, where they have been, and what kinds of products or

<sup>4</sup> Anthony Freda, *Private IP vs Public IP: What’s the Difference?*, AVG (June 4, 2021), <https://www.avg.com/en/signal/public-vs-private-ip-address>.

<sup>5</sup> *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), <https://www.accudata.com/blog/ip-targeting/>.

<sup>6</sup> *Location-Based Targeting That Puts You in Control*, CHOOZLE, <https://choozle.com/geotargeting-strategies/>.

<sup>7</sup> Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29, 2023), <https://tinyurl.com/c2ne77ua>.

<sup>8</sup> *IP Targeting: Understanding This Essential Marketing Tool*, ACCUDATA (Nov. 20, 2023), <https://www.accudata.com/blog/ip-targeting/>.

<sup>9</sup> Trey Titone, *The Future Of IP Address As An Advertising Identifier*, AD TECH EXPLAINED (May 16, 2022), <https://adtechexplained.com/the-future-of-ip-address-as-an-advertising-identifier/>.

1 services will appeal to their needs.”<sup>10</sup> For example, for a job fair in specific city, companies can send  
 2 advertisements to only those in the general location of the upcoming event.<sup>11</sup>

3 44. “IP targeting is a highly effective digital advertising technique that allows you to  
 4 deliver ads to specific physical addresses based on their internet protocol (IP) address. IP targeting  
 5 technology works by matching physical addresses to IP addresses, allowing advertisers to serve ads  
 6 to specific households or businesses based on their location.”<sup>12</sup>

7 45. “IP targeting capabilities are highly precise, with an accuracy rate of over 95%. This  
 8 means that advertisers can deliver highly targeted ads to specific households or businesses, rather  
 9 than relying on more general demographics or behavioral data.”<sup>13</sup>

10 46. In addition to “reach[ing] their target audience with greater precision,” businesses are  
 11 incentivized to use a customer’s public IP address because it “can be more cost-effective than other  
 12 forms of advertising.”<sup>14</sup> “By targeting specific households or businesses, businesses can avoid  
 13 wasting money on ads that are unlikely to be seen by their target audience.”<sup>15</sup>

14 47. In addition, “IP address targeting can help businesses to improve their overall  
 15 marketing strategy.”<sup>16</sup> “By analyzing data on which households or businesses are responding to their  
 16 ads, businesses can refine their targeting strategy and improve their overall marketing efforts.”<sup>17</sup>

17 48. The collection of IP addresses here is particularly invasive here given that OpenX and  
 18

19 <sup>10</sup> See, e.g., *The Essential Guide to Geomarketing: Strategies, Tips & More*, DEEP SYNC (Nov. 20,  
 20 2023), <https://deepsync.com/geomarketing/>.

21 <sup>11</sup> See, e.g., *Personalize Your Website And Digital Marketing Using IP Address*, GEOFLI,  
 22 [https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-](https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns)  
 23 [marketing-campaigns](https://geofli.com/blog/how-to-use-ip-address-data-to-personalize-your-website-and-digital-marketing-campaigns).

24 <sup>12</sup> *IP Targeting*, SAVANT DSP, [https://www.savantdsp.com/ip-targeting?gad\\_source=1&gclid=Cj](https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB)  
 25 [0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV](https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB)  
 26 [5-5maUaAgtNEALw\\_wcB](https://www.savantdsp.com/ip-targeting?gad_source=1&gclid=Cj0KCQjw1Yy5BhD-ARIsAI0RbXZJKJSqMI6p1xAxyqai1WhAiXRJTbX8qYhNuEvIfSCJ4jfOV5-5maUaAgtNEALw_wcB).

27 <sup>13</sup> *Id.*

28 <sup>14</sup> Herbert Williams, *The Benefits of IP Address Targeting for Local Businesses*, LINKEDIN (Nov. 29,  
 29 2023), [https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-](https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf)  
 30 [williams-z7bhf](https://www.linkedin.com/pulse/benefits-ip-address-targeting-local-businesses-herbert-williams-z7bhf).

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

1 a number of the entities the Third Parties sync with and whose trackers Defendant also installs on  
 2 Website users' browsers<sup>18</sup> are data brokers. As a report from NATO found:

3 [a] data broker may receive information about a[] [website] user,  
 4 including his ... IP address. The user then opens the [website] while  
 5 his phone is connected to his home Wi-Fi network. When this  
 6 happens, the data broker can use the IP address of the home network  
 7 to identify the user's home, and append this to the unique profile it  
 8 is compiling about the user. If the user has a computer connected to  
 9 the same network, this computer will have the same IP address. The  
 10 data broker can then use the IP address to connect the computer to  
 11 the same user, and identify that user when their IP address makes  
 12 requests on other publisher pages within their ad network. Now the  
 13 data broker knows that the same individual is using both the phone  
 14 and the computer, which allows it to track behaviour across devices  
 15 and target the user and their devices with ads on different  
 16 networks.<sup>19</sup>

17 49. In other words, not only does the collection of IP addresses by the Third Parties cause  
 18 harm in and of itself, data brokers like OpenX and a number of the entities the Third Parties sync  
 19 with and whose trackers Defendant also installs on Website users' browsers can use IP addresses to  
 20 identify users, append the IP address to a unique profile containing even more information about the  
 21 user, specifically attaches IP addresses to comprehensive user profiles, and track Plaintiff and Class  
 22 Members across the Internet using their IP addresses and compiling vast reams of other personal  
 23 information in the process.

24 50. For these reasons, under Europe's General Data Protection Regulation, IP addresses  
 25 are considered "personal data, as they can potentially be used to identify an individual."<sup>20</sup>

26 51. Likewise, under the California Consumer Privacy Act, IP addresses are considered  
 27 "personal information" because they are "reasonably capable of being associated with, or could  
 28

<sup>18</sup> As detailed herein, those entities include but are not limited to Experian/Tapad, TransUnion/Neustar, Lotame, and LiveRamp (the "Linked Data Brokers").

<sup>19</sup> HENRIK TWETMAN & GUNDARS BERGMANIS-KORATS, NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE, DATA BROKERS AND SECURITY at 11 (2020), [https://stratcomcoe.org/cuploads/pfiles/data\\_brokers\\_and\\_security\\_20-01-2020.pdf](https://stratcomcoe.org/cuploads/pfiles/data_brokers_and_security_20-01-2020.pdf).

<sup>20</sup> IS AN IP ADDRESS PERSONAL DATA?, CONVESIO, <https://convesio.com/knowledgebase/article/is-an-ip-address-personal-data/>; *see also* WHAT IS PERSONAL DATA?, EUROPEAN COMMISSION, [https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data\\_en](https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_en)

1 reasonably be linked, directly or indirectly, with a particular consumer or household.” Cal. Civ.  
 2 Code § 1798.140(v)(1)(A).<sup>21</sup>

3 **B. The Trackers Are “Pen Registers” That Defendant And The Third**  
 4 **Parties Use To De-Anonymize And Identify Users And Sell Their**  
 5 **Information To Advertisers**

6 52. When companies build their websites, they install or integrate various third-party  
 7 scripts into the code of the website in order to collect data from users or perform other functions.<sup>22</sup>

8 53. Often times, third-party scripts are installed on websites “for advertising purposes.”<sup>23</sup>

9 54. Further, “[i]f the same third-party tracker is present on many sites, it can build a more  
 10 complete profile of the user over time.”<sup>24</sup>

11 55. Defendant has long incorporated the Trackers’ code into the code of its Website,  
 12 including when Plaintiff and Class Members visited the Website. Thus, when Plaintiff visited the  
 13 Website, the Website caused the Trackers to be installed on Plaintiff’s and other users’ browsers.

14 56. As described below, when a user visits the Website, the Website’s code—as  
 15 programmed by Defendant—installs the Trackers onto the user’s browser. This allows the Third  
 16 Parties—through their respective Trackers—to collect Plaintiff’s and Class Members’ IP addresses  
 17 and Device Metadata, and pervasively track them across the Internet.

18 57. The Trackers also causes additional data points to be sent from Plaintiff’s and Class  
 19 Members’ browser to the Third Parties, which are meant to uniquely identify users across sessions  
 20 and devices. In addition to the public IP address, key elements include the user-agent string (browser,  
 21 operating system, and device type) and device capabilities such as supported image formats and

22 <sup>21</sup> A “consumer” is defined as “a natural person who is a California resident.” Cal. Civ. Code  
 23 § 1798.140(i.) A “household” is defined as “a group ... of consumers who cohabitate with one  
 24 another at the same residential address and share use of common devices or services.” Cal. Civ.  
 25 Code § 1798.140(1).)

26 <sup>22</sup> See *Third-party Tracking*, PIWIK, <https://piwik.pro/glossary/third-party-tracking/> (“Third-party  
 27 tracking refers to the practice by which a tracker, other than the website directly visited by the user,  
 28 traces or assists in tracking the user’s visit to the site. Third-party trackers are snippets of code that  
 are present on multiple websites. They collect and send information about a user’s browsing history  
 to other companies...”).

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*



compression methods. Persistent identifiers like the PUID, GUID, UID, PSVID, and User-Agent ensure users can be tracked even after clearing standard session data like cookies. Advanced methods like fingerprinting and server-side matching remain unaffected by cookie deletion. Combined, these elements form a detailed, unique fingerprint that allows for cross-site tracking and behavioral profiling.

58. Defendant and the Third Parties then use the public IP addresses, Device Metadata, and other information of Website visitors that are collected and set by the Trackers, including those of Plaintiff and Class Members, to deanonymize Plaintiff and Class Members, serve hyper-targeted advertisements, and unjustly enrich themselves through this improperly collected information.

59. At no time prior to the installation and use of the Trackers on Plaintiff's and Class Members's browsers, or prior to the use of the Trackers, did Defendant procure Plaintiff's and Class Members's consent for such conduct. Nor did Defendant obtain a court order to install or use the Trackers.

*1. The ADNXS Tracker And The Data Broker Partners It  
Cookie Syncs With*

60. Microsoft is a technology company with software-as-a-service products, such as Microsoft Advertising. Microsoft owns and operates the ADNXS Tracker, which it provides to website owners like Defendant for a fee. Microsoft rebranded ADNXS to "Microsoft Invest," but the two are the same service.

61. The ADNXS Tracker is a "demand-side platform," which is explained in more detail below. According to Microsoft, the ADNXS Tracker is "a strategic buying platform built for the needs of today's advertisers looking to invest in upper-funnel buying and drive business results."<sup>25</sup>

62. Microsoft facilitates the selling of Defendant's Website users to interested advertisers, who will bid to show those users advertisements targeted to their identity through this Tracker. This process enables Defendant to monetize its Website. To achieve this, Microsoft uses its Tracker to

---

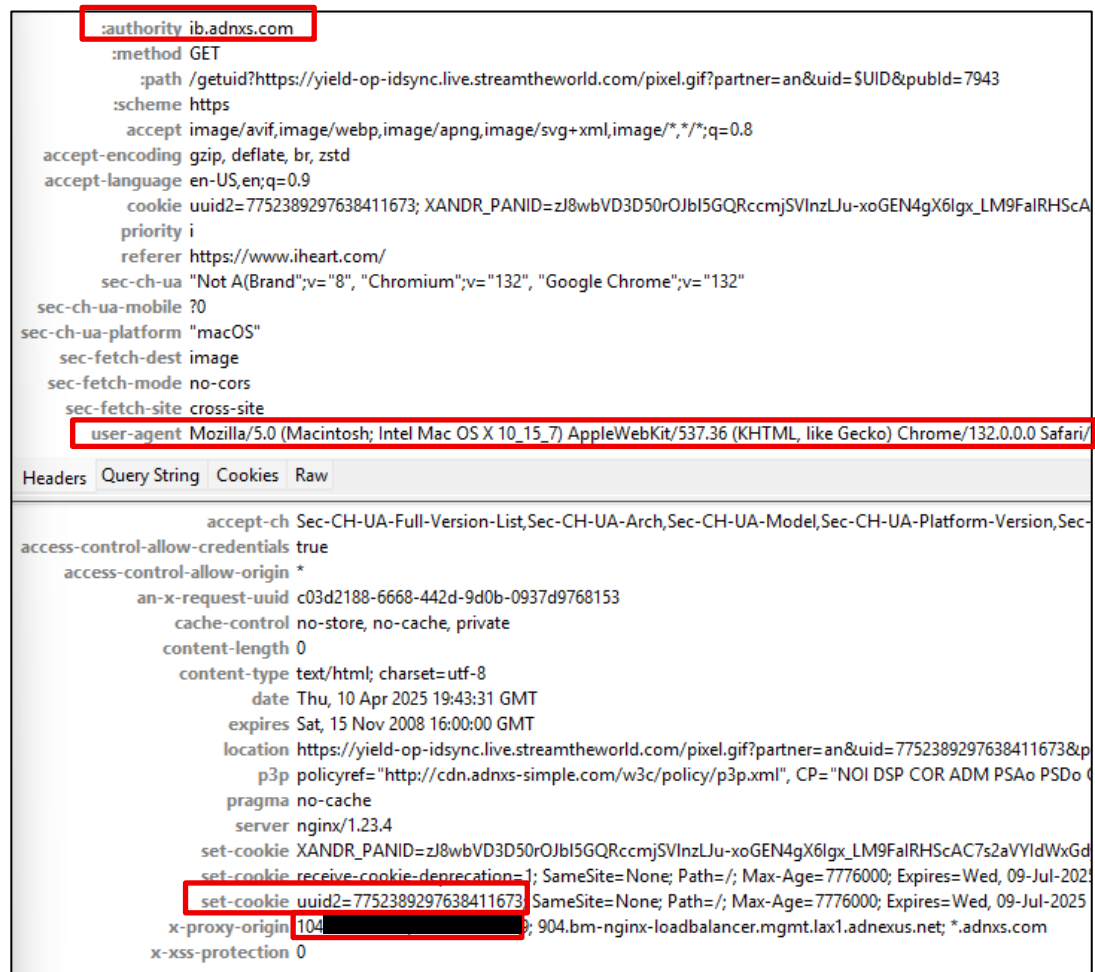
<sup>25</sup> *About Microsoft Invest*, MICROSOFT IGNITE (Feb. 12, 2024), <https://learn.microsoft.com/en-us/xandr/invest/about-invest>.



1 receive, store, and analyze information collected from website visitors, such as visitors of  
2 Defendant's Website.

3 63. When a user visits Defendant's Website, the user's browser sends an HTTP request  
4 to Defendant's server, and Defendant's server sends an HTTP response with directions to install the  
5 ADNXS Tracker on the user's browser. The ADNXS Tracker, in turn, instructs the user's browser  
6 to send Microsoft the user's IP address and Device Metadata—which Microsoft records—as the  
7 below screenshot of traffic from Plaintiff's browser indicates (relevant portions highlighted in red  
8 boxes).<sup>26</sup>

9 **Figure 4:**



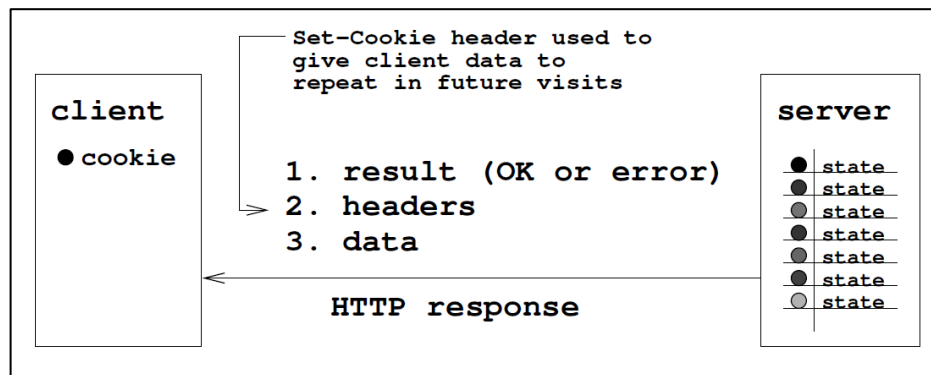
27 <sup>26</sup> All but the first three digits of Plaintiff's IP address (104) have been redacted throughout this  
28 Complaint to protect her privacy.

64. Moreover, Microsoft stores a cookie (the unique identifier, “UUID2” in Figure 4 above) with the user’s IP address and Device Metadata in the user’s browser cache. The UUID2 “[r]egisters a unique ID that identifies a returning user’s device” that “is used for targeted ads.”<sup>27</sup>

65. When the user subsequently visits Defendant’s Website, the ADNXS Tracker locates the UUID2 stored on the user’s browser. If the cookie is stored on the browser, the ADNXS Tracker causes the browser to send the UUID2 along with the user’s IP address and Device Metadata to Microsoft.

66. Using the UUID2, IP addresses, and Device Metadata, Microsoft can track and identify Website users across the Internet. A general diagram of this process is pictured as Figure 5, which explains how the Website causes the ADNXS Tracker to install a cookie on the user’s browser and instructs the user’s browser to send the user’s IP address and Device Metadata along with the UUID2.

**Figure 5:**



67. If the user clears his or her cookies, then the user wipes out the ADNXS Tracker from its cache. Accordingly, the next time the user visits Defendant’s Website the process begins over again: (i) Defendant’s server installs the ADNXS Tracker on the user’s browser, (ii) the ADNXS Tracker instructs the browser to send Microsoft the user’s IP address and Device Metadata, (iii) the ADNXS Tracker stores a UUID2 value in the browser cache, and (iv) Microsoft will continue to receive the user’s IP address, Device Metadata on subsequent Website visits along with the UUID2.

<sup>27</sup> FREEMAN CLARKE, COOKIE POLICY, <https://www.freemanclarke.com/en-us/cookie-policy/>

68. In all cases, however, Microsoft receives a user's IP address, Device Metadata, UUID2 every time its Tracker is loaded by the Website.

69. In addition to the UUID2, the ADNXS Tracker also sets the "XANDR\_PANID," which "registers data on the visitor" and "is used to optimize advertisement relevance."<sup>28</sup>

**Figure 6:**

```
set-cookie XANDR_PANID=zJ8wbVD3D50rOJbI5GQRccmjSVlnzLJu-xoGEN4gX6lqx_LM9FaIRH5cAC7s2aVYldWxGdykzEPHviMq_PCqth7l6DrsRCBK3WjL7fmtINE
```

70. The ADNXS Tracker will also share the user's UUID2 value with many of the Linked Data Brokers on the Website. The explicit purpose of this process—which is called "cookie syncing" and is alleged in more detail below—is to identify the user by matching that user with any profiles Microsoft and/or these other third parties may have on the user, which are then provided by Microsoft for sale to advertisers.

**(i) Experian/Tapad**

71. For example, Microsoft syncs its UUID2 with the Tapad tracker, which Defendant also installs on Website users' browsers. As the below screenshot from Plaintiff's browser indicates, the value of the "adnxs\_uid" parameter matches the value of the UUID2 parameter in Figure 4. Indeed, "APPNEXUS" is mentioned in the transmission. Tapad is also enhancing the information Microsoft knows about Plaintiff with information that Tapad knows about Plaintiff (and vice versa), something indicated by the path of the GET request, "idsync." Finally, Tapad is installing its own cookies (the unique identifiers "TapAd\_TS," "TapAd\_DID" and "TapAd\_3WAY\_SYNCs") on Plaintiff's browser for further tracking, syncing and de-anonymization.

**Figure 7:**

```
:authority pixel.tapad.com
:method GET
:path /idsync/appnexus/ceivethenpush?adnxs_uid=7752389297638411673&gdpr=0&gdpr_consent=
:scheme https
accept image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding gzip, deflate, br, zstd
accept-language en-US,en;q=0.9
cookie TapAd_TS=1738644090222; TapAd_DID=da343462-30cc-413b-bcf4-adaecc7b7b6c; TapAd_3WAY_SYNCs=1!2419-2!2142-3!2142
priority i
referer https://acdn.adnxs.com/
sec-ch-ua "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"
```

<sup>28</sup> EY, COOKIE POLICY, [https://www.ey.com/en\\_ce/legal-and-privacy/cookie-policy](https://www.ey.com/en_ce/legal-and-privacy/cookie-policy)

72. Tapad is a registered data broker in California<sup>29</sup> and is owned by Experian,<sup>30</sup> another registered data broker.<sup>31</sup> The purpose of Tapad’s tracker—which is owned and operated by these entities and used in conjunction with Experian’s services—is to perform identity resolution. As Experian describes it:

[i]dentity resolution matches fragmented identifiers to a single profile. This creates a unified, cross-channel view of a consumer that helps marketers understand a customer’s demographics, lifestyle, interests, and where and how they engage with your brand. Identity resolution improves campaign targeting and enables marketers to deliver personalized marketing messages.<sup>32</sup>

73. Tapad identifies users by “crunching 150 billion data points—from cookies, cellphone IDs (which link individual phones to app downloads and Web browsing), Wi-Fi connections, website registrations, browsing history and other inputs.”<sup>33</sup> Tapad then aggregates these inputs into what it called a “Device Graph,” which allows advertisers to connect individuals to all the devices those individuals use for the purpose of delivering targeted advertisements.<sup>34</sup>

74. Tapad integrates with Experian’s “offline consumer data set (purchase behaviors, interests, lifestyle info).”<sup>35</sup> This includes “first-party data such as names, physical addresses, email addresses, mobile ad identifiers (MAIDs), IP addresses, and other information.”<sup>36</sup> And as Experian advertisers, its identity graph is composed of “[o]ver 250M individuals and 126 million households,”

<sup>29</sup> DATA BROKER REGISTRATION FOR TAPAD, INC., <https://oag.ca.gov/data-broker/registration/187511>.

<sup>30</sup> Allison Schiff, *Telenor Sells Tapad to Experian for \$280 Million*, ADEXCHANGER (Nov. 19, 2020), <https://www.adexchanger.com/privacy/telenor-sells-Tapad-to-experian-for-280-million/>.

<sup>31</sup> DATA BROKER REGISTRATION FOR EXPERIAN INFORMATION SOLUTIONS, INC., <https://oag.ca.gov/data-broker/registration/186691>.

<sup>32</sup> <https://www.experian.com/marketing/consumer-sync/identity-resolution>.

<sup>33</sup> *Id.*

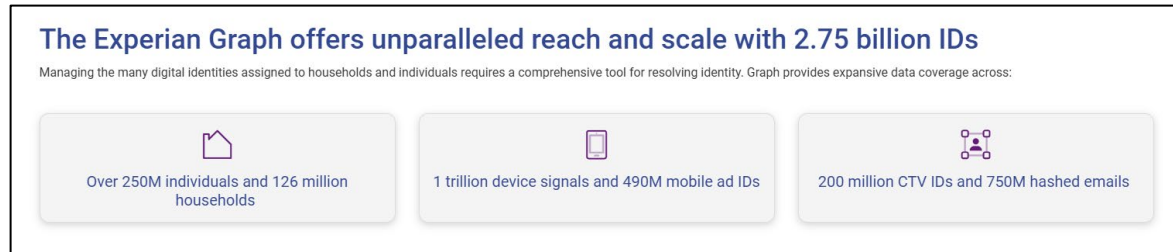
<sup>34</sup> <https://techcrunch.com/2016/02/01/telenor-jumps-into-ad-tech-acquires-Tapad-for-360m/>.

<sup>35</sup> Anthony Vargas, *How Experian Is Using Tapad To Build New ID Resolution And Analytics Products*, ADEXCHANGER (Feb. 1, 2023), <https://www.adexchanger.com/data-exchanges/how-experian-is-using-tapad-to-build-new-id-resolution-and-analytics-products/>.

<sup>36</sup> SHERMAN, *supra*, at 6 (cleaned up); *see also* EXPERIAN, OMNIIMPACT, <https://tinyurl.com/mve5jb65>.

enabling its partners like Microsoft to “known and anonymous IDs and data back to a single person or household to resolve identity.”<sup>37</sup>

**Figure 8:**



75. Thus, when Microsoft partners with advertisers to bid on Website users—as is the ADNXS Tracker’s function as a demand-side platform—advertisers can better identify and target their bids as a result of the ADNXS Tracker syncing with Tapad’s tracker, which de-anonymizes and identifies users. Tapad and Experian, in turn, build on their already expansive database through this transaction. And Defendant profits from installing both trackers on its Website because its users can be sold to advertisers for more money, thus enriching Defendant.

**(ii) Lotame**

76. As another example, Microsoft syncs its UUID2 with the Crowd Control (or “crwdcntrl”) tracker, which is developed and operated by Lotame, a registered data broker in California.<sup>38</sup> In March 2025, Lotame was acquired by Epsilon,<sup>39</sup> another data broker.<sup>40</sup> Defendant also installs this tracker on Website users’ browsers.

77. As the below screenshot from Plaintiff’s browser indicates, the value of the “tpid=” parameter matches the value of the UUID2 parameter in Figure 4. Indeed, the value of the “tp” parameter is even identified to be “ANXS.” Lotame is also enhancing the information Microsoft knows about Plaintiff with information that Lotame knows about Plaintiff (and vice versa),

<sup>37</sup> GRAPH | EXPERIAN’S IDENTITY GRAPH, <https://www.experian.com/marketing/consumer-sync/identity-resolution/identity-graph>.

<sup>38</sup> DATA BROKER REGISTRATION FOR LOTAME SOLUTIONS, INC., <https://oag.ca.gov/data-broker/registration/186954>.

<sup>39</sup> Epsilon, *Publicis To Acquire Lotame The World’s Leading Independent End-To-End Data Solution* (Mar. 6, 2025), <https://www.epsilon.com/us/about-us/pressroom/lotame-acquisition>.

<sup>40</sup> DATA BROKER REGISTRATION FOR EPSILON MANAGEMENT, LLC, <https://oag.ca.gov/data-broker/registration/186453>.

something indicated by the path of the GET request, “sync.” Finally, Lotame is installing its own cookies on Plaintiff’s browser (the “cc\_id”) for further tracking, syncing, and de-anonymization.

**Figure 9:**

```

:authority sync.crowdctrl.net
:method GET
:path /qmap?c=2816&tp=ANXS&tpid=7752389297638411673&gdpr=&gdpr_consent=
:scheme https
accept image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
accept-encoding gzip, deflate, br, zstd
accept-language en-US;q=0.9
cookie _cc_id=13df8fe33740df6f5d11a4472944cb3a; _cc_dc=3; _cc_aud="ABR4nGNgYGBI%2FzQADjAwMiv5AGgAq1QKF"; _cc_cc=
priority i
referer https://acdn.adnxs.com/
sec-ch-ua "Not A(Brand";v="8", "Chromium";v="132", "Google Chrome";v="132"

```

78. Lotame claims to operate a “Data Management Platform” or “DMP.” A Data Management Platform is a sophisticated technology tool used in the field of advertising (AdTech) and marketing (MarTech) to collect, analyze, and leverage data for better audience targeting and campaign optimization. It serves as a centralized data hub that consolidates and organizes vast amounts of user information from various sources.”<sup>41</sup>

79. “At its core, a DMP collects first-party, second-party, and third-party data ... Once the data is collected, the DMP employs advanced algorithms and machine learning techniques to analyze and segment the audience. It helps marketers understand their customers’ behaviors, preferences, and interests, enabling them to create more personalized and targeted marketing campaigns.”<sup>42</sup>

80. “By leveraging a DMP, marketers can deliver more personalized and relevant experiences to their target audience, resulting in higher engagement and conversion rates. They can optimize their advertising spend, minimize wastage, and achieve better marketing outcomes.”<sup>43</sup>

81. Lotame takes first party data and uses it to match a company’s audience against Lotame’s comprehensive user profiles. That is, Lotame analyzes a company’s first party data “for traits that your customers have in common and build[s] out that initial audience using Lotame’s

<sup>41</sup> Saurav Das, *Data-Management-Platform (DMP) – Simplified?*, MEDIUM (June 17, 2023), <https://medium.com/@101writer/what-is-dmp-d9aa6fcfe057>.

<sup>42</sup> *Id.*

<sup>43</sup> *Id.*

1 lookalike modeling capabilities to include new customers who also have those characteristics,”  
2 making that information more valuable to advertisers, thereby driving Defendant’s revenue.<sup>44</sup>

3 82. Lotame offers such advertisers the ability to “[e]xpand and enrich your target  
4 audiences with scalable, trusted partner data” sources via their exclusive partnerships.<sup>45</sup> In other  
5 words, Lotame compiles comprehensive user profiles by tracking users across the Internet so  
6 customers like Defendant can “get maximum value from your first-party data” to “drive audience  
7 growth” and target advertising campaigns to boost revenue.<sup>46</sup>

8 83. “Audience targeting involves breaking down consumers into specific segments based  
9 on the data you’ve collected about them and their behavior, such as their interests, demographics and  
10 buying history. Then, you’ll use that information to tailor your marketing messages directly to that  
11 segment for more powerful engagement and, ideally, greater conversions.”<sup>47</sup>

12 84. Lotame does this through its proprietary identity resolution tool called the “Panorama  
13 Graph.” The “Lotame Panorama Graph, our patented identity resolution engine, consists of a variety  
14 of signals including email, cookies, and device IDs as well as machine learning models to uniquely  
15 deliver both accuracy and scale. It unlocks addressability to 1.3 billion users with global coverage.  
16 Find your people around the world and make meaningful, respectful connections that last.”<sup>48</sup>

17 85. Lotame can then use these individual profiles to provide marketers, such as  
18 Defendant, “with fresher, more relevant and addressable audiences” which “translates into better 1:1  
19 targeting and personalization.”<sup>49</sup> Indeed, Lotame admits that “[i]dentity resolution and activation  
20

21  
22 <sup>44</sup> Alexandra Theriault, *First-Party Data vs Third-Party Data: How To Use Them*, LOTAME (Nov.  
23 21, 2024), <https://www.lotame.com/resources/1st-party-2nd-party-3rd-party-data-what-does-it-all-mean/>.

24 <sup>45</sup> *Data Informed Audiences*, LOTAME, <https://web.archive.org/web/20250115002619/https://spherical.lotame.com/data-informed-audiences/> (as accessed Jan. 15, 2025).

25 <sup>46</sup> *Id.*

26 <sup>47</sup> Danielle Smith, *How Does Audience Targeting Work?* LOTAME (July 24, 2024), <https://www.lotame.com/resources/finding-target-audience/>.

27 <sup>48</sup> *Panorama Graph*, LOTAME, <https://tinyurl.com/5byy9tns> (as accessed Feb. 13, 2025).

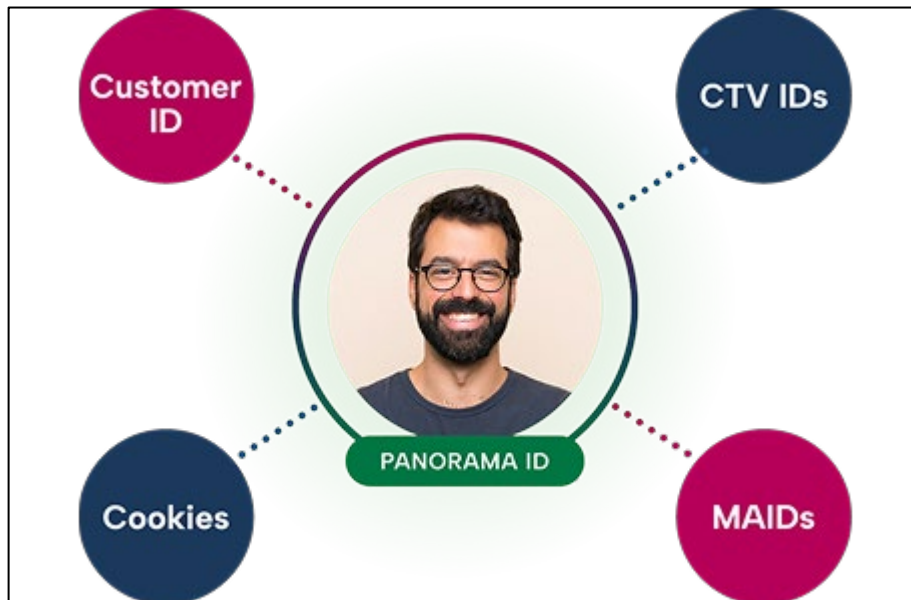
28 <sup>49</sup> *Id.*



1 help marketers identify unique users across various channels and devices in order to deliver  
2 personalized advertising messages that drive outcomes.”<sup>50</sup>

3 86. “Lotame Panorama ID is a global pseudonymous identifier that represents a single  
4 consumer view across channels. Built from multiple inputs, our publisher-adopted ID resolves a  
5 variety of user signals, such as email and digital data from web, mobile, and CTV. Unlike other  
6 identifiers, Panorama ID is proven to ensure data-driven audience activation works in cookie and  
7 cookie-restricted environments.”<sup>51</sup> Indeed, “Panorama Graph connects and unifies consumer digital  
8 touch points across emails, cookies, and device IDs to offer a single view of a user.”<sup>52</sup>

9 **Figure 10:**



10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20 87. Lotame touts that as a result of these efforts, “Lotame’s data collaboration solutions  
21 help data sellers maximize the value of your rich online and offline datasets.”<sup>53</sup>

22 **(iii) TransUnion/Neuster**

23 88. As a final example, Microsoft syncs its UUID2 with the AGKN tracker, which is  
24 operated by TransUnion, and whose tracker Defendant also installs on Website users’ browsers. As

25 <sup>50</sup> *Id.*

26 <sup>51</sup> *Lotame Panorama ID*, LOTAME, <https://tinyurl.com/zhav4j2w> (as accessed Mar. 24, 2025).

27 <sup>52</sup> *Lotame Panorama Identity*, LOTAME, <https://tinyurl.com/y2bm9xyf> (as accessed Jan. 2, 2025).

28 <sup>53</sup> *Data Sellers*, LOTAME, <https://tinyurl.com/yfzwwnmX> (as accessed Jan. 2, 2025).



the below screenshot from Plaintiff's browser indicates, the value of the "adnxsid" parameter matches the value of the UUID2 parameter in Figure 4. TransUnion is also enhancing the information Microsoft knows about Plaintiff with information that TransUnion knows about Plaintiff, and vice versa. Finally, TransUnion is installing its own cookies (the unique identifier "ab") on Plaintiff's browser for further tracking, syncing and de-anonymization.

**Figure 11:**



89. In October 2013, Neustar, a registered data broker in California,<sup>54</sup> purchased Aggregate Knowledge (AGKN) for \$119 million. This combined Neustar's "access to a large dataset of telephone numbers and location data through relationships with major ISPs and wireless carriers" and "geo-targeted online advertising" with AGKN's "ability to help clients allocate media dollars, and expand cross-sell opportunities with marketers and agencies."<sup>55</sup>

90. In or about December 2021, TransUnion, who is also a registered data broker in California,<sup>56</sup> acquired Neustar for \$3.1 billion. The press release stated Neustar was "a premier identity resolution company ... [that] enables customers to build connected consumer experiences by combining decision analytics with real-time identity resolution services driven by its OneID™ platform."<sup>57</sup> Thus, "Neustar Marketing Solutions is now part of TransUnion TruAudience,"

<sup>54</sup> DATA BROKER REGISTRATION FOR NEUSTAR, INC., <https://oag.ca.gov/data-broker/registration/562353>.

<sup>55</sup> Zach Rodgers, *Neustar Acquires DMP Aggregate Knowledge For \$119M*, ADEXCHANGER (Oct. 30, 2013), <https://www.adexchanger.com/data-exchanges/neustar-acquires-aggregate-knowledge-for-119m/>.

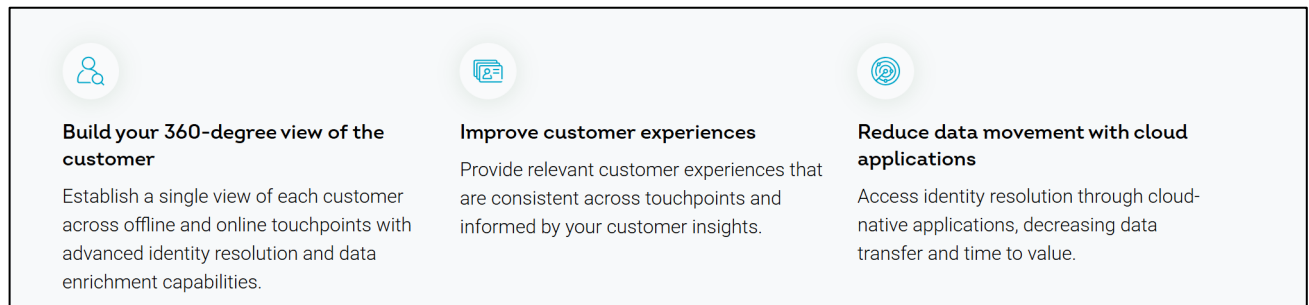
<sup>56</sup> DATA BROKER REGISTRATION FOR TRANSUNION DIGITAL LLC, <https://oag.ca.gov/data-broker/registration/562235>.

<sup>57</sup> TRANSUNION AND NEUSTAR ANNOUNCE TRANSACTION CLOSE, <https://newsroom.transunion.com/transunion-and-neustar-announce-transaction-close/>

“Neustar Fraud Solutions is now part of TransUnion TruValidate,” and “Neustar Communications Solutions is now part of TransUnion TruContact.”<sup>58</sup>

91. Neustar’s services, as integrated with TransUnion’s, enable advertisers to target specific people. This is done through TruAudience Identity Solutions, which “[e]stablish a single view of each customer across offline and online touchpoints with advanced identity resolution and data enrichment capabilities.”<sup>59</sup> Indeed, TruAudience “[e]nhance[s] your view of the customer with fresh contact information and predictive demographic data for insights, audience building, and engagement,” which can be compiled into a “first-party identity graph to power prospecting, media monetization, or agency operations.”<sup>60</sup>

**Figure 12:**



92. TruAudience also allows website operators like Defendant to “[c]reate audiences using your first-party data, third-party audiences, and/or TransUnion’s marketing attributes.” Defendant can then “[m]ake the most of [its] first party data assets with advanced identity resolution and audience building capabilities, alongside a broad distribution network,” and “[a]ccess audiences from trusted third-party data providers to reach your ideal customers across all verticals.”<sup>61</sup> This

<sup>58</sup> Neustar, <https://home.neustar/>.

<sup>59</sup> TRUAUDIENCE IDENTITY SOLUTIONS, <https://www.transunion.com/solution/truaudience/identity>.

<sup>60</sup> *Id.*

<sup>61</sup> AUDIENCE SOLUTIONS, <https://www.transunion.com/solution/truaudience/audiences>. For clarity, “[f]irst-party data is collected directly from a company's own customers through platforms like websites, mobile apps, or physical stores ... Third-party data is procured from external data brokers and aggregators, providing information about consumers but without a direct relationship between the data collector and the consumer.” Derek Andersen, *What Marketers Need to Know About 1st, 2nd, and 3rd-Party Data*, INVOCA BLOG (Mar. 3, 2025), <https://www.invoca.com/blog/marketers-need-to-know-first-second-third-party-data>.

1 includes “[u]sing TransUnion data,”<sup>62</sup> which is obviously extensive given TransUnion’s size and  
2 other credit reporting services.

3 93. In other words, the purpose of TransUnion’s services are to provide as much  
4 information about a user from as many sources as possible to advertisers, such that the user is de-  
5 anonymized and has a plethora of personal and demographic information attached to them when  
6 offered up for sale. TransUnion does this through the AGKN tracker, which links the information  
7 the tracker collects about the user from the Website with TransUnion’s vast repository of data. That  
8 information is then shared or synced with Microsoft’s ADNXS Tracker to enable better targeting by  
9 advertisers. And better targeting means advertisers will pay more money to show advertisements to  
10 Defendant’s users, which enriches Defendant at the cost of its users’ privacy.

11 \* \* \*

12 94. This is a non-exhaustive list of the Linked Data Brokers with whom Microsoft syncs  
13 its ADNXS Tracker. Suffice it to say, Microsoft is syncing its ADNXS Tracker with registered data  
14 brokers and data sellers to collect as much information about a user as possible and de-anonymize  
15 the user, all of which is used for advertising purposes and to enrich Defendant without users’ consent.

16 95. The ADNXS Tracker is at least a “process” because it is “software that identifies  
17 consumers, gathers data, and correlates that data.” *Greenley*, 684 F. Supp. 3d at 1050.

18 96. Further, the ADNXS Tracker is a “device” because “in order for software to work, it  
19 must be run on some kind of computing device.” *See, e.g., James v. Walt Disney Co.*, 701 F. Supp.  
20 3d 942, 952 (N.D. Cal. 2023)

21 97. Because the ADNXS Tracker captures outgoing “routing, addressing, and signaling”  
22 information—the IP address, Device Metadata, and unique user IDs—from visitors to the Website,  
23 it is a “pen register” for the purposes of CIPA § 638.50(b).

24 98. The ADNXS Tracker is also a “pen register” because the information it records is  
25 being used to ascertain the identity of “visitors to Defendant’s [W]ebsite,” and is thus recording  
26

27 \_\_\_\_\_  
28 <sup>62</sup> *Id.*

“addressing” information. *Heiting*, 2025 WL 736594, at \*3; *see also Greenley*, 684 F. Supp. 3d at 1050 (“software that identifies consumers” is a pen register).

## 2. *The TripleLift Tracker And The Data Broker Partners It Cookie Syncs With*

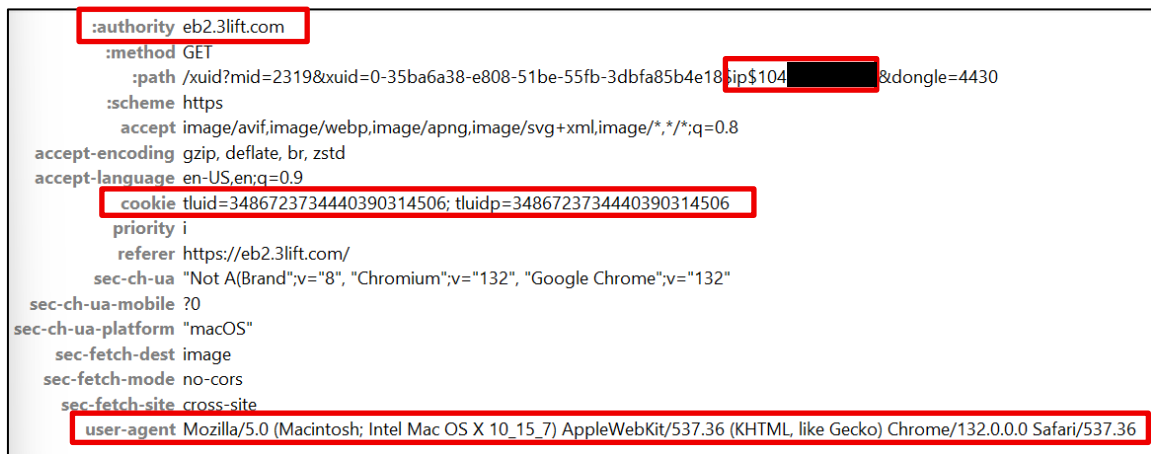
99. TripleLift is a software-as-a-service company that develops and operates the TripleLift Tracker, which it provides to website owners, like Defendant, for a fee. As described in more detail below, TripleLift is a “supply-side platform.”

100. According to TripleLift, its “technology powers ads that make advertising better for everyone—higher performing for brands, more lucrative for publishers and more respectful of the consumer’s experience.”<sup>63</sup>

101. In other words, TripleLift enables companies to sell their user inventory to advertisers, thereby earning revenue. To achieve this, TripleLift uses its Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant’s Website.

102. When a user visits Defendant’s Website, the user’s browser sends an HTTP request to Defendant’s server, and Defendant’s server sends an HTTP response with directions to install the TripleLift Tracker on the user’s browser. The TripleLift Tracker, in turn, instructs the user’s browser to send TripleLift the user’s IP address and Device Metadata—which the TripleLift Tracker records—as indicated in the below screenshot of Plaintiff’s browser traffic on the iHeart Website (relevant portions highlighted in red boxes).

**Figure 13:**



<sup>63</sup> *Technology*, TRIPLELIFT, <https://triplelift.com/technology>

1           103. Moreover, TripleLift stores unique user identifiers in the user’s browser cache (the  
2 unique identifiers, “TLUID” and “TLUIDP,” in Figure 13). The TLUID “is used to identify web  
3 browsers across sites and over time for ad serving purposes.”<sup>64</sup> The TLUIDP “is used to identify  
4 web browsers on a top-level domain over time for ad serving purposes *in situations where third party*  
5 *cookies are disabled.*”<sup>65</sup> That is, when Defendant installs TripleLift’s Tracker, TripleLift can still  
6 track and identify users to sell their information, even if users have purportedly blocked cookies.

7           104. When the user subsequently visits Defendant’s Website, the TripleLift Tracker  
8 locates these unique identifiers stored on the user’s browser. If these unique identifiers are stored on  
9 the browser, the TripleLift Tracker causes the browser to send the unique identifiers along with the  
10 user’s IP address and Device Metadata to TripleLift.

11           105. If the user clears his or her cookies, then the user wipes out the TripleLift Tracker  
12 from its cache. Accordingly, the next time the user visits Defendant’s Websites, the process begins  
13 over again: (i) Defendant installs the TripleLift Tracker on the user’s browser, (ii) the TripleLift  
14 Tracker instructs the browser to send TripleLift the user’s IP address and Device Metadata, (iii) the  
15 TripleLift Tracker stores unique user identifiers in the browser cache, and (iv) TripleLift will  
16 continue to receive the user’s IP address and Device Metadata on subsequent visits to the Websites  
17 along with the unique user identifiers.

18           106. In all cases, however, TripleLift receives a user’s IP address, Device Metadata, and  
19 unique user ID every time its Tracker is loaded by the Websites. Using the IP addresses, Device  
20 Metadata, and unique user IDs, TripleLift can track and identify Website users across the Internet.

21           107. As TripleLift notes, its Tracker is designed to “[s]ynchronize IDs with partners in  
22 order to solicit bids from demand partners [*e.g.*, advertisers], which we do to sell the advertising  
23 space of our supply partners [*e.g.*, websites like Defendant’s].” This allows TripleLift and its  
24 partners to understand that [] two different identifiers relate to the same device.”<sup>66</sup>

25  
26 <sup>64</sup> EY, *COOKIE POLICY*, [https://www.ey.com/en\\_ce/legal-and-privacy/cookie-policy](https://www.ey.com/en_ce/legal-and-privacy/cookie-policy)

27 <sup>65</sup> *Id.*

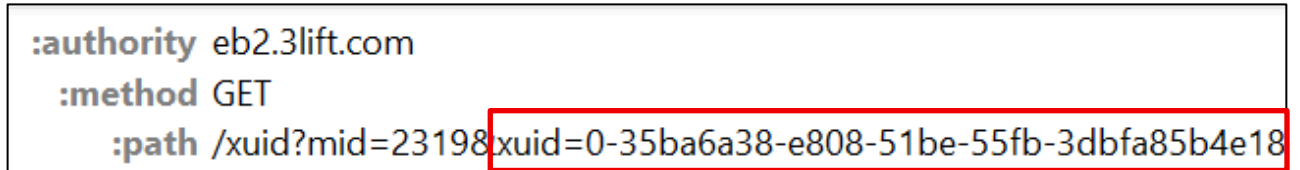
28 <sup>66</sup> TRIPLELIFT PLATFORM PRIVACY NOTICE, <https://triplelift.com/platform-privacy-policy/>

108. The explicit purpose of this process—which is called “cookie syncing” and is described in more detail below—is to identify the user by matching that user with any profiles TripleLift and/or these Linked Data Brokers may have on the user, which are then provided by TripleLift for sale to advertisers.

(i) **Lotame**

109. In addition to the TLUIDP and TLUID unique identifiers, TripleLift also sets or syncs with the unique identifier “xuid.” The purpose of this identifier is to enable TripleLift to “connect with” “a DSP or demand partner.”<sup>67</sup>

**Figure 14:**



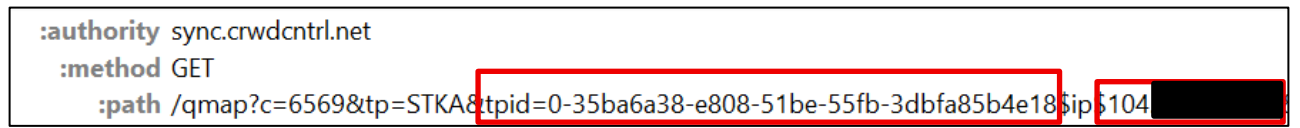
A screenshot of a browser request to `eb2.3lift.com`. The request details are as follows:

- Authority:** `eb2.3lift.com`
- Method:** `GET`
- Path:** `/xuid?mid=23198&xuid=0-35ba6a38-e808-51be-55fb-3dbfa85b4e18`

The `xuid` parameter value is highlighted with a red box.

110. Syncing with this same “xuid” is Lotame, whose capabilities are described above. As the below screenshot from Plaintiff’s browser traffic indicates the value of the “xuid” parameter in Figure 14 above—which is recorded in a transmission to the TripleLift Tracker—matches the value of the “tpid” parameter in the transmission to Lotame’s Crowd Control tracker. Through this transmission, Lotame also received and recorded Plaintiff’s IP address.

**Figure 15:**



A screenshot of a browser request to `sync.crowdctrl.net`. The request details are as follows:

- Authority:** `sync.crowdctrl.net`
- Method:** `GET`
- Path:** `/qmap?c=6569&tp=STKA&tpid=0-35ba6a38-e808-51be-55fb-3dbfa85b4e18&ip=104.15.104.104`

The `tpid` parameter value is highlighted with a red box, matching the `xuid` value in Figure 14. The IP address is also visible at the end of the path.

111. As described above, Lotame maintains extensive profiles on “1.3 billion users,”<sup>68</sup> which “help data sellers maximize the value of your rich online and offline datasets.”<sup>69</sup> Thus, Lotame is de-anonymizing Plaintiff by syncing their unique identifiers to Lotame’s repository of information, and then providing that information to TripleLift for sale to advertisers. Through this process, TripleLift learns everything Lotame knows about the user (and vice versa), and Lotame is enriching

<sup>67</sup> DEMAND PARTNERS, <https://docs.triplelift.com/docs/demand-partners>.

<sup>68</sup> *Panorama Graph*, LOTAME, <https://tinyurl.com/5byy9tns> (as accessed Feb. 13, 2025).

<sup>69</sup> *Data Sellers*, LOTAME, <https://tinyurl.com/yfzwwnmX> (as accessed Jan. 2, 2025).

1 the value of the information TripleLift sells to advertisers. This causes advertisers to place higher  
 2 bids to show advertisements to Website users, thus enriching Defendant at the expense of Website  
 3 users' privacy.

4 \* \* \*

5 112. This is a non-exhaustive list of the entities with whom TripleLift syncs its Tracker.  
 6 Suffice it to say, TripleLift is syncing its Tracker with registered data brokers and data sellers to  
 7 collect as much information about a user as possible and de-anonymize the user, all of which is used  
 8 for advertising purposes and to enrich Defendant without users' consent.

9 113. The TripleLift Tracker is at least a "process" because it is "software that identifies  
 10 consumers, gathers data, and correlates that data." *Greenley*, 684 F. Supp. 3d at 1050.

11 114. Further, the TripleLift Tracker is a "device" because "in order for software to work,  
 12 it must be run on some kind of computing device." *See, e.g., James*, 701 F. Supp. 3d 942, 952 (N.D.  
 13 Cal. 2023)

14 115. Because the TripleLift Tracker captures outgoing "routing, addressing, and signaling"  
 15 information—the IP address, Device Metadata, and unique user IDs—from visitors to the Website,  
 16 it is a "pen register" for the purposes of CIPA § 638.50(b).

17 116. The TripleLift Tracker is also a "pen register" because the information it records is  
 18 being used to ascertain the identity of "visitors to Defendant's [W]ebsite," and is thus recording  
 19 "addressing" information. *Heiting*, 2025 WL 736594, at \*3; *see also Greenley*, 684 F. Supp. 3d at  
 20 1050 ("software that identifies consumers" is a pen register).

21 3. *The OpenX Tracker And The Data Broker Partners It Cookie*  
 22 *Syncs With*

23 117. OpenX is a registered data broker in California<sup>70</sup> that helps companies like Defendant  
 24 "utilize their [first party] data, leverage [third party data], and package up audiences for marketers  
 25 that will drive ad revenue."<sup>71</sup>

26 <sup>70</sup> DATA BROKER REGISTRATION FOR OPENX TECHNOLOGIES, INC., [https://oag.ca.gov/data-broker/](https://oag.ca.gov/data-broker/registration/193614)  
 27 registration/193614.

28 <sup>71</sup> *OpenAudience*, OPENX, <https://www.openx.com/why-openx/openaudience/>

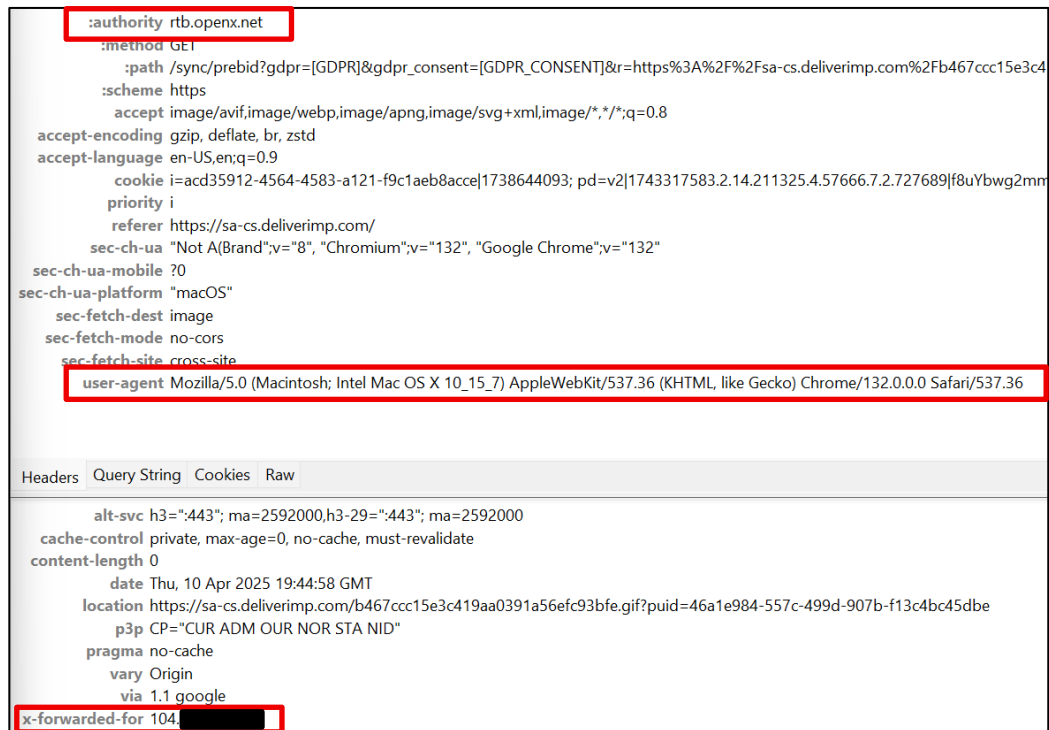


118. OpenX takes this data and uses it to “match [a company’s] audience against [OpenX’s] graph to put users in audience segments that [OpenX] mak[es] available to marketers.”<sup>72</sup>

119. In other words, OpenX compiles comprehensive user profiles by tracking users across the Internet. OpenX then enriches the information of its client’s end users (like Defendant’s end users) with the profile data to make that information more valuable to advertisers by aggregating that information into a graph, thereby driving Defendant’s revenue. To achieve this, OpenX uses its OpenAudience Tracker to receive, store, and analyze information collected from website visitors, such as visitors of Defendant’s Website.

120. When a user visits Defendant’s Website, the user’s browser sends an HTTP request to Defendant’s server, and Defendant’s server sends an HTTP response with directions to install the OpenX Tracker on the user’s browser. The OpenX Tracker, in turn, instructs the user’s browser to send Microsoft the user’s IP address and Device Metadata—which OpenX records—as the below screenshot of traffic from Plaintiff’s browser indicates (relevant portions highlighted in red boxes):

**Figure 16:**



<sup>72</sup> *Data Activation*, OPENX, <https://www.openx.com/why-openx/openaudience/>.



121. Moreover, OpenX stores at least two cookies (the unique identifiers, “i” and “univ\_id” in the screenshot below) with the user’s IP address and Device Metadata in the user’s browser cache.

**Figure 17:**

| Name    | Value   |
|---------|---|
| i       | acd35912-4564-4583-a121-f9c1aeb8acce1738644093                      |
| pd      | v2 1743317583.2.14.211325.4.57666.7.2.727689 f8uYbwg2mmeS.wivJwwwlw |
| univ_id | 537072971a5bee045-83e5-4230-85f2-3edc45c46b571744314293295913       |

122. When the user subsequently visits Defendant’s Websites, the OpenX Tracker locates these unique identifiers stored on the user’s browser. If the unique identifiers are stored on the browser, the OpenX Tracker causes the browser to send the unique identifiers along with the user’s IP address and Device Metadata to OpenX. A general diagram of this process is pictured as Figure 5, which explains how the Websites cause the OpenX Tracker to install a cookie on the user’s browser and instructs the user’s browser to send the user’s IP address and Device Metadata along with the unique identifiers.

123. If the user clears his or her cookies, then the user wipes out the OpenX Tracker from its cache. Accordingly, the next time the user visits Defendant’s Website the process begins over again: (i) Defendant’s server installs the OpenX Tracker on the user’s browser, (ii) the OpenX Tracker instructs the browser to send OpenX the user’s IP address and Device Metadata, (iii) the OpenX Tracker stores unique identifiers in the browser cache, and (iv) OpenX will continue to receive the user’s IP address and Device Metadata on subsequent Website visits along with the unique identifiers.

124. In all cases, however, OpenX receives a user’s IP address, Device Metadata, and unique user identifiers information every time its Tracker is loaded Websites.

125. Through its “univ\_id” unique identifier, OpenX syncs its vast repository of user profiles with a variety of the Linked Data Brokers whose trackers Defendant also installs on Website users’ browsers. OpenX thus enhances the information being bought by and sold to advertisers,

enabling greater targeting, leading to higher bids, and enriching Defendant at the expense of Website users' privacy.

(i) **Microsoft, TripleLift, Experian, And Lotame**

126. As initial examples, OpenX syncs its "univ\_id" identifier with four of the third party trackers whose capabilities are described above: Microsoft (the ADNXS Tracker), TripleLift, Experian (the Tapad tracker), and Lotame (the Crowd Control tracker). As the below traffic from Plaintiff's browser indicates, the "univ\_id" in Figure 17 is identical to the highlighted value being recorded by the aforementioned third parties in each of the screenshots below:

**Figure 18:**

|            |  |
|------------|--|
| :authority | ib.adnxs.com   |
| :method    | GET  |
| :path      | /setuid?entity=82&code=a5bee045-83e5-4230-85f2-3edc45c46b57&gdpr=0&gdpr_consent= |

|            |   |
|------------|---|
| :authority | eb2.3lift.com   |
| :method    | GET   |
| :path      | /xuid?mid=3658&xuid=a5bee045-83e5-4230-85f2-3edc45c46b57&dongle=0cfd&gdpr=0&gdpr_consent= |

|            |   |
|------------|---|
| :authority | pixel.tapad.com   |
| :method    | GET   |
| :path      | /idsync/ex/receive?partner_id=1830&partner_device_id=a5bee045-83e5-4230-85f2-3edc45c46b57 |

|            |   |
|------------|---|
| :authority | sync.crowdctrl.net  |
| :method    | GET   |
| :path      | /map/c=10620/tp=TRAD/tpid=a5bee045-83e5-4230-85f2-3edc45c46b57/gdpr=0/gdpr_consent= |

127. Through this process, OpenX shares its vast repository of information and whatever it knows about Plaintiff with each of these four third parties (and vice versa) Lotame's repository of information, and then providing that information to TripleLift for sale to advertisers. Through this process, TripleLift learns everything Lotame knows about the user (and vice versa), and Lotame is enriching the value of the information TripleLift sells to advertisers. This causes advertisers to place higher bids to show advertisements to Website users, thus enriching Defendant at the expense of Website users' privacy.

(ii) **LiveRamp**

128. As another example, OpenX syncs its "univ\_id" with the RLCDN tracker, which is also installed by Defendant on Website users' browsers. The RLCDN tracker is owned and operated

by LiveRamp, another registered data broker in California.<sup>73</sup> As the below screenshot from Plaintiff's browser indicates, the value of the "partner\_uid" parameter matches the value of the "univ\_id" parameter in Figure 17. LiveRamp is also enhancing the information OpenX knows about Plaintiff with information that LiveRamp knows about Plaintiff (and vice versa), something indicated by the name of the GET request, "idsync." Finally, LiveRamp is installing its own cookies on Plaintiff's browser for further tracking, syncing, and de-anonymization.

**Figure 19:**



129. LiveRamp provides "identity resolution," which "[b]ring in data from across identity spaces" "to enable the delivery of more personali[z]ed and meaningful customer experiences."<sup>74</sup>

130. LiveRamp claims to "maintain[] the largest and most accurate people-based identity graph on the market."<sup>75</sup> Its identity graph has PII or personally identified information "on 245 million individuals in the U.S."<sup>76</sup>

131. LiveRamp does this through its "LiveRamp Identity Graph," which "is a people-based map connecting de-identified offline touchpoints and online devices" that (i) "[r]esolv[es] separate emails, postal addresses, and phone numbers to a single individual"; (ii) "[m]atch[es] disparate

<sup>73</sup> DATA BROKER REGISTRATION FOR LIVERAMP, INC., <https://oag.ca.gov/data-broker/registration/560496>.

<sup>74</sup> IDENTITY RESOLUTION, LIVERAMP, <https://liveramp.uk/identity-resolution/>.

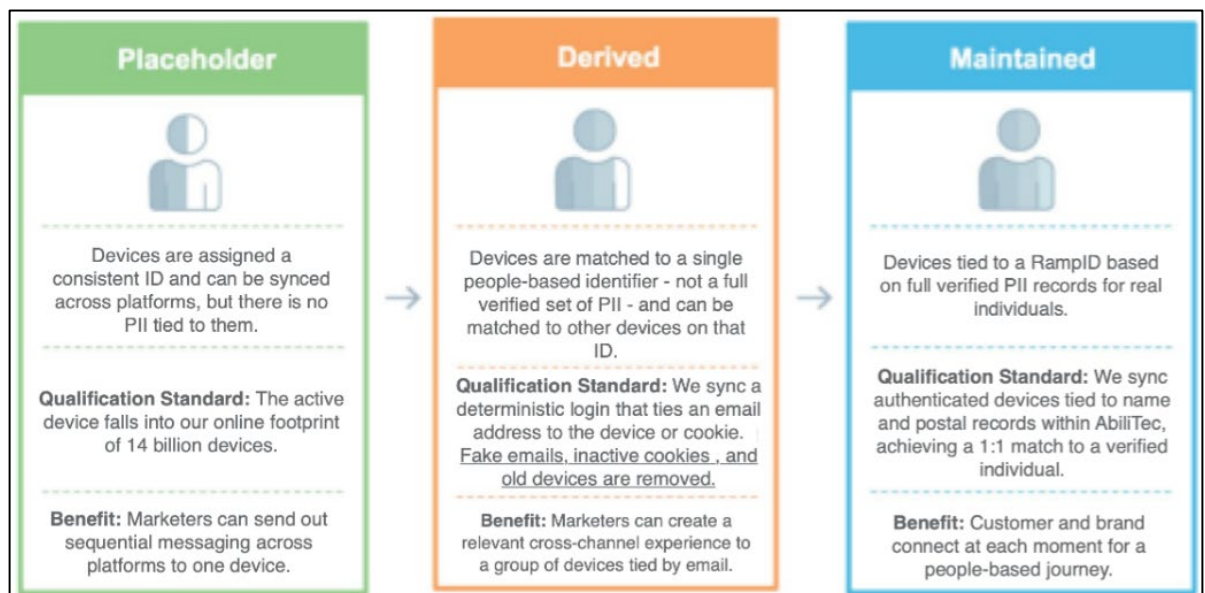
<sup>75</sup> INTERPRETING RAMPID, LIVERAMP'S PEOPLE BASED IDENTIFIER, LIVERAMP, <https://tinyurl.com/jpmtx3ut>.

<sup>76</sup> *Id.*

1 devices to people-based pseudonymous identifiers”; and (iii) “[m]erg[es] these offline and online  
2 identity spaces into a unified ... people-based ID space.”<sup>77</sup>

3 132. LiveRamp collects individuals’ “PII touchpoints” or personally identifiable  
4 information such as their “email [addresses], name[s] and postal [addresses], [and] phone  
5 [numbers].”<sup>78</sup> “[I]deally LiveRamp will always have all PII touchpoints merged for an individual,  
6 but our algorithms will only merge this data when we are extremely confident they are tied to the  
7 same individual.”<sup>79</sup>

8 **Figure 20:**



18 133. For that reason, LiveRamp sets a RampID on the user’s browser, which “enables real-  
19 time people-based insights” to be attached to each visitor.<sup>80</sup> LiveRamp does this by taking a  
20 company’s first-party data, and seamlessly matching it to RampID, LiveRamp’s “people-based  
21 identity graph.”<sup>81</sup>

22  
23  
24 <sup>77</sup> RAMPID METHODOLOGY, <https://docs.liveramp.com/identity/en/rampid-methodology.html>

25 <sup>78</sup> INTERPRETING RAMPID, LIVERAMP’S PEOPLE-BASED IDENTIFIER, <https://tinyurl.com/jpmtx3ut>.

26 <sup>79</sup> *Id.*

27 <sup>80</sup> *Id.*

28 <sup>81</sup> *Id.*



141. As alleged herein, the Trackers are designed to conduct targeted advertising and boost Defendant's revenue, all through their surreptitious collection of Plaintiff's and Class Members' personal information.

142. To put the invasiveness of Defendant's violations of the CIPA into perspective, it is also important to understand three concepts: data brokers, real-time bidding, and cookie syncing.

143. In short, the import of these concepts is that: (i) the Third Parties are data brokers (or partner with data brokers) that collect user information from Website visitors to uniquely identify and de-anonymize users by combining their IP addresses, Device Metadata, and unique user ID values with whatever information those Third Parties have on a user from other sources; (ii) the Third Parties share that information with other entities to create the most complete user profile they can (through cookie syncing), which includes a more complete and non-anonymous portrait of the user; and (iii) those profiles are offered up for sale through the real-time bidding process to the benefit of Defendant and the Third Parties and to the detriment of users' privacy interests.

#### **A. Data Brokers And Real-Time Bidding: The Information Economy**

##### *1. Data Brokers*

144. While "[t]here is no single, agreed-upon definition of data brokers in United States law,"<sup>82</sup> California law defines a "data broker" as "a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct [*i.e.*, consumer-facing] relationship," subject to certain exceptions. Cal. Civ. Code § 1798.99.80(c).

145. Any entity that qualifies as a "data broker" under California law must specifically register as such Cal. Civ. Code § 1798.99.82(a), which OpenX and a number of the entities the Third Parties sync with (Experian/Tapad, TransUnion/Neustar, Lotame, LiveRamp) do.

146. Some data brokers prefer to characterize themselves as "identity graph providers," but this is a distinction without a difference. "An identity graph provides a single unified view of customers and prospects based on their interactions with a product or website across a set of devices and identifiers. An identity graph is used for real-time personalization and advertising targeting for

---

<sup>82</sup> SHERMAN, *supra*, at 2.

millions of users.”<sup>83</sup> This is exactly what data brokers do, and indeed, the entities that provide identity graphs are by and large required to register as data brokers under California law. An “identity graph provider” is therefore just a euphemism for “data broker.”

147. “Data brokers typically offer pre-packaged databases of information to potential buyers,” either through the “outright s[ale of] data on individuals” or by “licens[ing] and otherwise shar[ing] the data with third parties.”<sup>84</sup> Such databases are extensive, and can “not only include information publicly available [such as] from Facebook but also the user’s exact residential address, date and year of birth, and political affiliation,” in addition to “inferences [that] can be made from the combined data.”<sup>85</sup>

148. For instance, the NATO report noted that data brokers collect two sets of information: “observed and inferred (or modelled).” The former “is data that has been collected and is actual,” such as websites visited.” Inferred data “is gleaned from observed data by modelling or profiling,” meaning what users may be *expected* to do. On top of this, “[b]rokers typically collect not only what they immediately need or can use, but hoover up as much information as possible to compile comprehensive data sets that might have some future use.”<sup>86</sup>

149. Likewise, a report by the Duke Sanford Cyber Policy Program “examine[d] 10 major data brokers and the highly sensitive data they hold on U.S. individuals.”<sup>87</sup> The report found that “data brokers are openly and explicitly advertising data for sale on U.S. individuals’ sensitive demographic information, on U.S. individuals’ political preferences and beliefs, on U.S. individuals’ whereabouts and even real-time GPS locations, on current and former U.S. military personnel, and on current U.S. government employees.”<sup>88</sup>

<sup>83</sup> IDENTITY GRAPHS ON AWS, <https://aws.amazon.com/neptune/identity-graphs-on-aws/>.

<sup>84</sup> SHERMAN, *supra*, at 2.

<sup>85</sup> Tehila Minkus et al., *The City Privacy Attack: Combining Social Media and Public Records for Detailed Profiles of Adults and Children*, COSN ’15: PROCEEDINGS OF THE 2015 ACM ON CONFERENCE ON ONLINE SOCIAL NETWORKS 71, 71 (2015), <https://dl.acm.org/doi/pdf/10.1145/2817946.2817957>.

<sup>86</sup> TWETMAN & BERGMANIS-KORATS, *supra*, at 11.

<sup>87</sup> SHERMAN, *supra*, at 1.

<sup>88</sup> *Id.*



1           150. This data collection has grave implications for Americans’ right to privacy. For  
 2 instance, “U.S. federal agencies from the Federal Bureau of Investigation [] to U.S. Immigration and  
 3 Customs Enforcement [] purchase data from data brokers—without warrants, public disclosures, or  
 4 robust oversight—to carry out everything from criminal investigations to deportations.”<sup>89</sup>

5           151. As another example:

6           Data brokers also hold highly sensitive data on U.S. individuals such  
 7 as race, ethnicity, gender, sexual orientation, immigration status,  
 8 income level, and political preferences and beliefs (like support for  
 9 the NAACP or National LGBTQ Task Force) that can be used to  
 10 directly undermine individuals’ civil rights. Even if data brokers do  
 11 not explicitly advertise these types of data (though in many cases  
 they do), everything from media reporting to testimony by a Federal  
 Trade Commission commissioner has identified the risk that data  
 brokers use their data sets to make “predictions” or “inferences”  
 about this kind of sensitive information (race, gender, sexual  
 orientation, etc.) on individuals.

12           This data can be used by commercial entities within the U.S. to  
 13 discriminately target goods and services, akin to how Facebook  
 14 advertising tools allow advertisers to exclude certain groups, such  
 as those who are identified as people with disabilities or those who  
 are identified as Black or Latino, from seeing advertisements. 59  
 15 Many industries from health insurance to life insurance to banking  
 to e-commerce purchase data from data brokers to run  
 16 advertisements and target their services.

17           ...

18           Given identified discrimination problems in machine learning  
 19 algorithms, there is great risk of these predictive tools only further  
 driving up costs of goods and services (from insurance to housing)  
 for minority groups.<sup>90</sup>

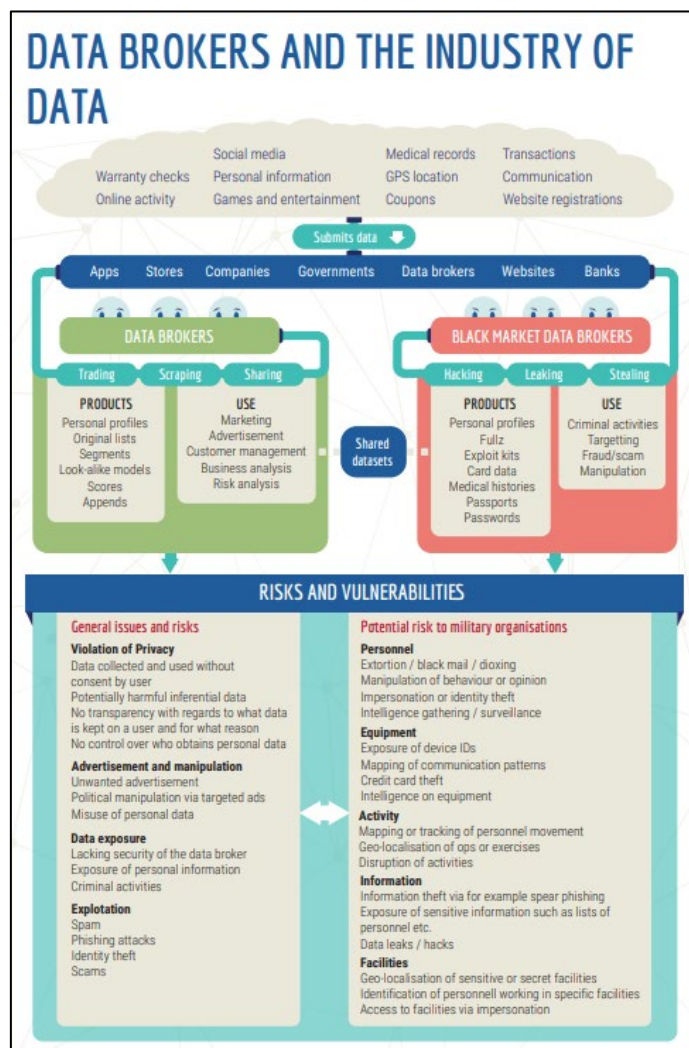
20           152. Similarly, as the report from NATO noted, corporate data brokers cause numerous  
 21 privacy harms, including but not limited to depriving users of the right to control who does and does  
 22 not acquire their personal information, unwanted advertisements that can even go as far as  
 23 manipulating viewpoints, and spam and phishing attacks.<sup>91</sup>

24  
 25  
 26 <sup>89</sup> *Id.* at 9.

27 <sup>90</sup> *Id.*

28 <sup>91</sup> TWETMAN & BERGMANIS-KORATS, *supra*, at 8.



**Figure 21:**

153. As noted above, data brokers, like OpenX and the Linked Data Brokers whose trackers Defendant installs on Website users' browsers, are able to compile such wide swaths of information in part by collecting users' IP addresses and Device Metadata, which is used by data brokers, like OpenX and the other data brokers the Third Parties sync with and whose trackers Defendant installs on Website users' browsers, to track users across the Internet.<sup>92</sup>

154. Indeed, as McAfee (a data security company) notes, "data brokers can ... even place trackers or cookies on your browsers ... [that] track your IP address and browsing history, which third parties can exploit."<sup>93</sup>

<sup>92</sup> *Id.* at 11.

<sup>93</sup> Jasdev Dhaliwal, *How Data Brokers Sell Your Identity*, MCAFEE (June 4, 2024), <https://www.mcafee.com/blogs/tips-tricks/how-data-brokers-sell-your-identity/>.

1           155. These data brokers will then:

2           take that data and pair it with other data they've collected about you,  
3           pool it together with other data they've got on you, and then share  
4           all of it with businesses who want to market to you. They can  
5           eventually build large datasets about you with things like: "browsed  
6           gym shorts, vegan, living in Los Angeles, income between \$65k-  
7           90k, traveler, and single." Then, they sort you into groups of other  
8           people like you, so they can sell those lists of like-people and  
9           generate their income.<sup>94</sup>

10           156. In short, by collecting IP addresses and Device Metadata, data brokers, like OpenX  
11           and the Linked Data Brokers and whose trackers Defendant installs on Website users' browsers,  
12           track users across the Internet, compiling various bits of information about users, building  
13           comprehensive user profiles that include an assortment of information, interests, and inferences, and  
14           offering up that information for sale to the highest bidder. The "highest bidder" is a literal term, as  
15           explained below.

16           157. As a result of Defendant's installation the trackers of these data brokers, the  
17           information of Plaintiff and Class Members is linked to any profiles these data brokers may have  
18           about them using their IP addresses and Device Metadata (or new profiles are created for Plaintiff  
19           and Class Members).

20           158. These profiles are then served up to any companies that want to advertise on  
21           Defendant's Website, and Defendant's users become more valuable as a result of having their IP  
22           addresses and Device Metadata linked to these data broker profiles. Thus, Defendant is unjustly  
23           enriched through advertising revenue by installing the Trackers on Plaintiff's and Class Members'  
24           browsers, and thus, enabling the Third Parties to collect Plaintiff's and Class Members' IP addresses  
25           and Device Metadata without consent.

## 26           2. *Real-Time Bidding*

27           159. Once data brokers like OpenX and the Linked Data Brokers collect Website users' IP  
28           addresses and Device Metadata, how do they "sell" or otherwise help Defendant monetize that  
information? This is where real-time bidding comes in.

---

<sup>94</sup> Paul Jarvis, *The Problem with Data Brokers: Targeted Ads and Your Privacy*, FATHOM ANALYTICS (May 10, 2022), <https://usefathom.com/blog/data-brokers>.

160. “Real Time Bidding (RTB) is an online advertising auction that uses sensitive personal information to facilitate the process to determine which digital ad will be displayed to a user on a given website or application.”<sup>95</sup>

161. “There are three types of platforms involved in an RTB auction: Supply Side Platforms (SSPs), Advertising Exchanges, and Demand Side Platforms (DSPs).” An SSP, which is at least one function of the TripleLift Tracker here,<sup>96</sup> “work[s] with website or app publishers to help them participate in the RTB process.” “DSPs [which is what the ADNXS Tracker is<sup>97</sup>] primarily work with advertisers to help them evaluate the value of user impressions and optimize the bid prices they put forth.”<sup>98</sup> And an Advertising Exchange “allows advertisers and publishers to use the same technological platform, services, and methods, and ‘speak the same language’ in order to exchange data, set prices, and ultimately serve an ad.”<sup>99</sup>

162. In other words, SSPs like the TripleLift Tracker provide user information to advertisers that might be interested in those users, DSPs like the ADNXS Tracker help advertisers select which users to advertise and target, and an Advertising Exchange is the platform on which all of this happens.

163. The RTB process works as follows:

After a user loads a website or app, an SSP [*e.g.*, TripleLift] will send user data to Advertising Exchanges ... The user data, often referred to as “bidstream data,” contains information like device identifiers, IP address, zip/postal code, GPS location, browsing history, location data, and more. After receiving the bidstream data, an Advertising Exchange will broadcast the data to several DSPs [*e.g.*, Microsoft]. The DSPs will then examine the broadcasted data to determine whether to make a bid on behalf of their client.

Ultimately, if the DSP wins the bid, its client’s advertisement will appear to the user. Since most RTB auctions are held on the

<sup>95</sup> Sara Geoghegan, *What is Real Time Bidding?*, ELECTRONIC PRIVACY INFORMATION CENTER (Jan. 15, 2025), <https://epic.org/what-is-real-time-bidding/>.

<sup>96</sup> TRIPLELIFT, THE CREATIVE SSP, <https://triplelift.com/>.

<sup>97</sup> MICROSOFT INVEST, <https://about.ads.microsoft.com/en/solutions/technology/microsoft-invest-dsp> (“Microsoft Invest is a demand-side platform built for the future of video advertising.”).

<sup>98</sup> Geoghegan, *supra*.

<sup>99</sup> *Introducing To Ad Serving*, MICROSOFT IGNITE (Mar. 3, 2024), <https://learn.microsoft.com/en-us/xandr/industry-reference/introduction-to-ad-serving>.

server/exchange side, instead of the client/browser side, the user only actually sees the winner of the auction and would not be aware of the DSPs who bid and lost. But even the losing DSPs still benefit because they also receive and collect the user data broadcasted during the RTB auction process. This information can be added to existing dossiers DSPs have on a user.<sup>100</sup>

**Figure 22:**

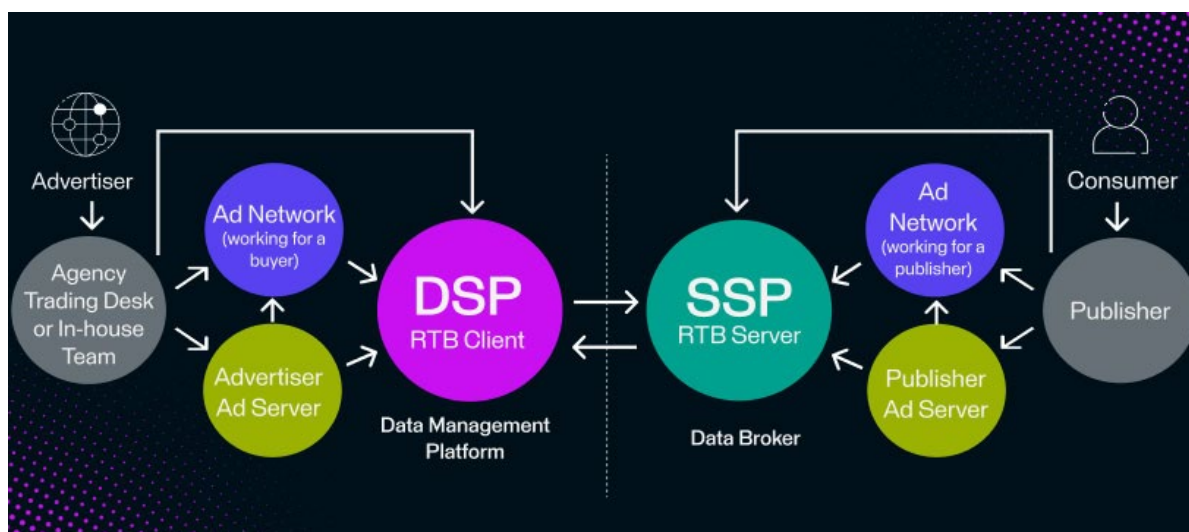


164. Facilitating this real-time bidding process means SSPs and DSPs must have as much information as possible about Defendant's users to procure the greatest interest from advertisers and the highest bids. These entities receive assistance because Defendant also installs the trackers of data brokers on its users' browsers:

the economic incentives of an auction mean that DSP [or SSP] with more specific knowledge of individuals will win desirable viewers due to being able to target them more specifically and out-bid other entities. As a consequence, the bid request is not the end of the road. The DSP enlists a final actor, the data management platform (DMP) [or a data broker]. DSPs [or SSPs] send bid requests to DMPs [and data brokers], who enrich them by attempting to identify the user in the request and use a variety of data sources, such as those uploaded by the advertiser, collected from other sources, or bought from data brokers. The DSP with the highest bid not only wins the right to deliver the ad—through the SSP—to the individual. The DSP also wins the right to cookie sync its own cookies with those from the [Advertising Exchange], thus enabling easier linkage of the data to the user's profile in the future.<sup>101</sup>

<sup>100</sup> Geoghegan, *supra*; see also REAL-TIME BIDDING, APPSFLYER, <https://www.appsflyer.com/glossary/real-time-bidding/>.

<sup>101</sup> Michael Veale & Federik Zuiderveen Borgesius, *Adtech and Real-Time Bidding under European Data Protection Law*, 23 GERMAN L. J. 226, 232-33 (2022) <https://tinyurl.com/yjddt5ey>.

**Figure 23:**

165. In other words, a SSP like TripeLift can solicit the highest bids for Website users by identifying and de-anonymizing those users by combining the information TripeLift knows about that user with the information other data brokers know about that user. If there is a match, then TripeLift will have significantly more information to provide about users, and that will solicit significantly higher bids from prospective advertisers (because the advertisers will have more information about the user to target their bids). Likewise, a DSP like Microsoft can generate the highest and most targeted bids from advertisers with providing those advertisers with as much information about users as possible, which it does by syncing with data brokers like Experian/Tapad, Lotame, TransUnion/Neustar, and OpenX—who in turn sync with even further data brokers and data sellers like the Linked Data Brokers.

166. All of this naturally enriches Defendant, as data on its users have now become more valuable thanks to the replete information the Third Parties are able to provide about users.

167. As the Federal Trade Commission (“FTC”) has noted, “[t]he use of real-time bidding presents potential concerns,” including but not limited to:

- (i) “incentiviz[ing] invasive data-sharing” by “push[ing] publishers [*i.e.*, Defendant] to share as much end-user data as possible to get higher valuation for their ad inventory—particularly their location data and cookie cache, which can be used to ascertain a person’s browsing history and behavior.”
- (ii) “send[ing] sensitive data across geographic borders.”



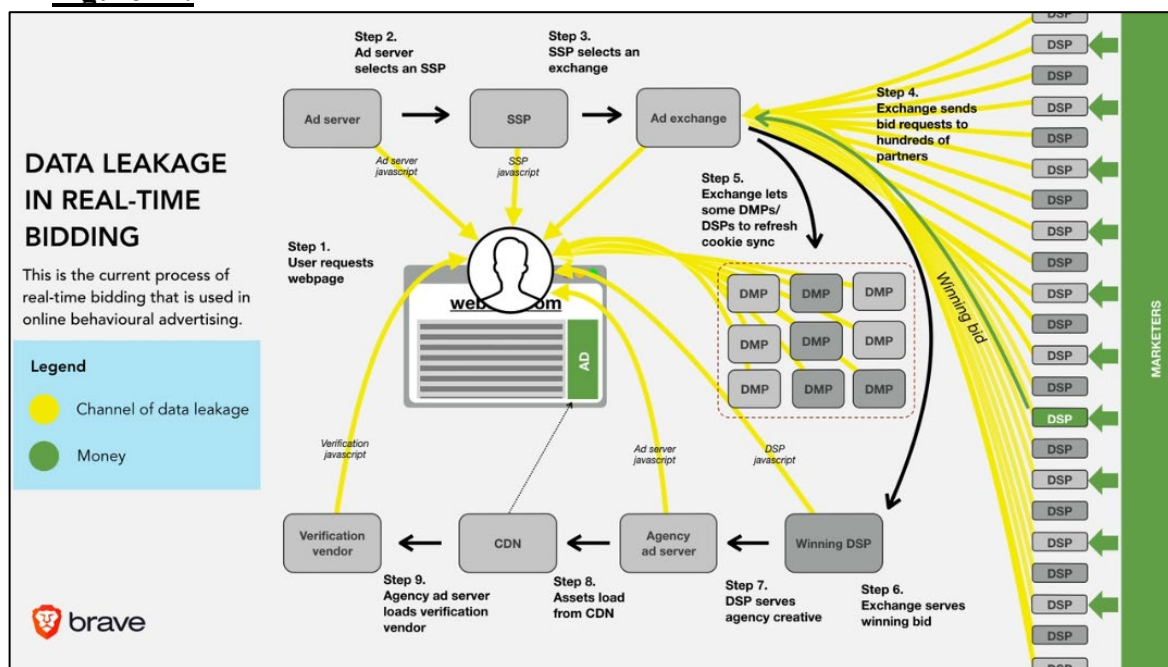
- (iii) sending consumer data “to potentially dozens of bidders simultaneously, despite only one of those parties—the winning bidder actually using that data to serve a targeted ad. Experts have previously cautioned that there are few (if any) technical controls ensuring those other parties do not retain that data for use in unintended ways.”<sup>102</sup>

168. Given Microsoft operates a DSP here, the last point is particularly relevant, as it means Microsoft—through the ADNXS Tracker—collects and discloses Website users’ information to *all prospective advertisers*, even if advertisers do not ultimately show a user an advertisement. This greatly diminishes the ability of users to control their personal information.

169. Likewise, the Electronic Privacy Information Center (“EPIC”) has warned that “[c]onsumers’ privacy is violated when entities disclose their information without authorization or in ways that thwart their expectations.”<sup>103</sup>

170. For these reasons, some have characterized “real-time bidding” as “[t]he biggest data breach ever recorded” because of the sheer number of entities that receive personal information<sup>104</sup>:

**Figure 24:**



<sup>102</sup> FEDERAL TRADE COMMISSION, UNPACKING REAL TIME BIDDING THROUGH FTC’S CASE ON MOBILEWALLA (Dec. 3, 2024), <https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/12/unpacking-real-time-bidding-through-ftcs-case-mobilewalla>.

<sup>103</sup> Geoghegan, *supra*.

<sup>104</sup> DR. JOHNNY RYAN, “RTB” ADTECH & GDPR, [https://assortedmaterials.com/rtb-evidence/\(video\)](https://assortedmaterials.com/rtb-evidence/(video)).

171. All of this is in line with protecting the right to determine who does and does not get to know one's information, a harm long recognized at common law and one the CIPA was enacted to protect against. *Ribas*, 38 Cal. 3d at 361 (noting the CIPA was drafted with a two-party consent requirement to protect "the right to control the nature and extent of the firsthand dissemination of [one's] statements"); *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press* 489 U.S. 749, 763-64 (1989) ("[B]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.").

### 3. Cookie Syncing

172. It should now be clear both the capabilities of the Third Parties (*i.e.*, data brokers who de-anonymize users, or companies who sync with data brokers for this purpose) and the reasons Defendant installs their Trackers on its Website (to sell to advertisers in real-time bidding with as much information about users as possible to solicit the highest bids). The final question is how do these Third Parties share information amongst each other and with others to offer the most complete user profiles up for sale? This occurs through "cookie syncing."

173. Cookie syncing is a process that "allow[s] web companies to share (synchronize) cookies, and match the different IDs they assign for the same user while they browse the web."<sup>105</sup> This allows entities like the Third Parties to circumvent "the restriction that sites can't read each other cookies, in order to better facilitate targeting and real-time bidding."<sup>106</sup>

174. Cookie syncing works as follows:

Let us assume a user browsing several domains like website1.com and website2.com, in which there are 3rd-parties like tracker.com and advertiser.com, respectively. Consequently, these two 3rd-parties have the chance to set their own cookies on the user's browser, in order to re-identify the user in the future. Hence, tracker.com knows the user with the ID user123, and advertiser.com knows the same user with the ID userABC.

<sup>105</sup> Panagiotis Papadopoulos et al., *Cookie Synchronization: Everything You Always Wanted to Know But Were Afraid to Ask*, 1 WWW '19: THE WORLD WIDE WEB CONFERENCE 1432, 1432 (2019), <https://dl.acm.org/doi/10.1145/3308558.3313542>.

<sup>106</sup> Gunes Acar et al., *The Web Never Forgets: Persistent Tracking Mechanisms in the Wild*, 6B CCS'14: ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 674, 674 (2014)



Now let us assume that the user lands on a website (say website3.com), which includes some JavaScript code from tracker.com but not from advertiser.com. Thus, advertiser.com does not (and cannot) know which users visit website3.com. However, *as soon as the code of tracker.com is called, a GET request is issued by the browser to tracker.com (step 1), and it responds back with a REDIRECT request (step 2), instructing the user's browser to issue another GET request to its collaborator advertiser.com this time, using a specifically crafted URL (step 3).*

...

When advertiser.com receives the above request along with the cookie ID userABC, it finds out that userABC visited website3.com. *To make matters worse, advertiser.com also learns that the user whom tracker.com knows as user123, and the user userABC is basically one and the same user.* Effectively, CSync enabled advertiser.com to collaborate with tracker.com, in order to: (i) find out which users visit website3.com, and (ii) *synchronize (i.e., join) two different identities (cookies) of the same user on the web.*<sup>107</sup>

**Figure 25:**



<sup>107</sup> Papadopoulos, *supra*, at 1433.



Website users as possible to create comprehensive user profiles. The Third Parties record IP Addresses, Device Metadata, and unique user IDs in the first instance, but those pieces of information are matched to comprehensive profiles held by these data brokers through “cookie syncing.” Also through “cookie syncing,” those profiles are shared amongst the Third Parties and with other entities to form the most fulsome picture with the most attributes as possible. And those profiles are offered up for sale to interested advertisers through real-time bidding using the Third Parties’ Trackers (and again through cookie syncing), where users will command more value the more advertisers know about a user.

180. Thus, the Third Parties enrich the value Defendant’s users would otherwise command by tying the data they obtain directly from users on the Website (*e.g.*, IP addresses, Device Metadata, unique user IDs) with comprehensive user profiles.

181. Accordingly, Defendant is using the Trackers in conjunction with the Third Parties to (i) de-anonymize users, (ii) offer its users up for sale in real-time bidding, and (iii) monetize its Website by installing the Trackers and allowing the Third Parties to collect as much information about Website users as possible (without consent).

182. Thus, Defendant is unjustly enriched through their installation and use of the Trackers, which causes data to be collected by Third Parties without Plaintiff’s and Class Members’ consent, and that enable the Third Parties to sell Defendant’s user inventory in an ad-buying system. In addition, Plaintiff and Class Members lost the ability to control their information, as their information ends up in the hands of data brokers, advertising inventory sellers, and a virtually unlimited number advertisers themselves without knowledge or consent.

**B. Defendant Uses The ADNXS Tracker For Targeted Advertising, Identity Resolution, And Data Monetization**

183. Microsoft describes its advertising services, which include the ADNXS or Microsoft Invest Tracker, as “a strategic buying platform built for the needs of today’s advertisers looking to invest in upper-funnel buying and drive business results.”<sup>113</sup>

---

<sup>113</sup> *About Microsoft Invest*, MICROSOFT IGNITE (Feb. 12, 2024), <https://learn.microsoft.com/en-us/xandr/invest/about-invest> (last visited Dec. 23, 2024).

184. The ADNXS Tracker is a DSP as noted above.

185. Microsoft collects data to help companies with their marketing; when the processing system “receives ad requests, [it] applies data to the request, receives bids, makes decisions, serves creatives, logs, auctions, etc.”<sup>114</sup>

186. In particular:

The Microsoft Advertising platform is a real-time bidding system and ad server. The main processing system is called the “impression bus.” The impression bus receives ad requests, applies data to the request, receives bids, makes decisions, serves creatives, logs auctions, etc.

Ad calls come in via our inventory supply partners: exchanges, SSPs, ad networks, and a few valued publishers.

...

Once we get the call, we overlay segment data from our server-side cookie store. Data is added to the cookie store either through Xandr segment pixels or by clients sending us a file of data. We also contact third-party data providers and overlay any available data.

We contact all of the bidders on our platform. The ad call includes whatever user data belongs to each bidder, and information about the inventory. Bidders have a certain number of milliseconds in which to respond with a bid and the creative they want to serve.

...

The impression bus decides which bid wins based on the amount of the bid, and any preferences the publisher has about what they want served on their page. If the call was client-side, Microsoft Advertising serves the ad. If it was server-side, Microsoft Advertising passes the bid and the location of the creative to the partner who will ultimately serve the ad.<sup>115</sup>

187. Microsoft Invest (*i.e.*, the ADNXS Tracker) provides “targeting, bidding algorithms, multi-currency support, and all the other features of a premium ad server.”<sup>116</sup> To do this, Microsoft utilizes data from its cookie store. The “[d]ata is added to the cookie store either through Microsoft

<sup>114</sup> *Id.*

<sup>115</sup> <https://learn.microsoft.com/en-us/xandr/invest/about-invest>

<sup>116</sup> *About Microsoft Invest*, MICROSOFT IGNITE (Feb. 12, 2024), <https://learn.microsoft.com/en-us/xandr/invest/about-invest>

Advertising segment pixels or by clients sending [them] a file of data. [They] also contact third-party data providers and overlay any available data.”<sup>117</sup>

188. As alleged above, Microsoft also integrates with the data brokers whose trackers Defendant installs on the Websites. This provides Microsoft to de-anonymize and identify Website users, which it provides to advertisers so those advertisers can best target their advertisements. And, because Defendant’s users have now been de-anonymized and identified, Defendant devices additional revenue from this process because advertisers will pay more to show advertisements to Defendant’s users.

189. In other words, when users visit Defendant’s Websites, Microsoft collects users’ IP addresses, Device Metadata, and unique identifiers through its ADNXS Tracker to provide to advertisers interested in showing an advertisement to Defendant’s Website users, enriching that information by integrating with the trackers of data brokers (and its own data), and ultimately enabling Defendant to monetize its Websites and maximize revenue by enabling Microsoft to collect as much information about Defendant’s users as possible.

**C. Defendant Uses the TripleLift Tracker For Targeted Advertising Identity Resolution, And Data Monetization**

190. In marketing speak, TripleLift claims to combine “actionable data, advanced targeting, and premium inventory, we empower publishers and brands to discover new opportunities, achieve measurable outcomes, and engage audiences seamlessly across every platform.”<sup>118</sup> In actuality, TripleLift is an SSP that enables website operators like Defendant to sell their user inventory to interested advertisers.

191. On the advertiser side, TripleLift’s “data & targeting technology, TripleLift Audiences, ensures [advertisers] reach the right audience with a robust library of audience segments, optimizing toward your desired KPIs.”<sup>119</sup> On the publisher side (*i.e.*, Defendant and other website

---

<sup>117</sup> *Id.*

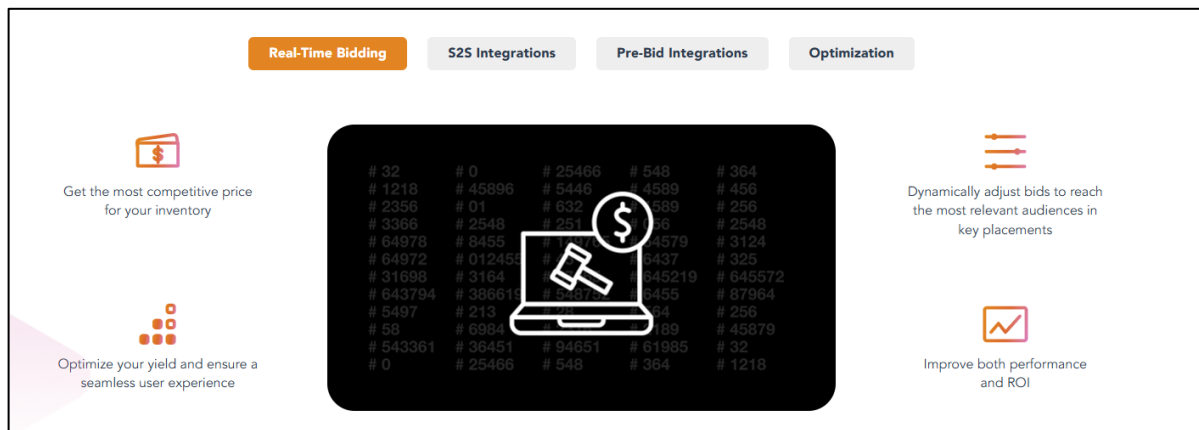
<sup>118</sup> CREATIVE THAT PERFORMS, TRIPLELIFT, <https://triplelift.com/about/>.

<sup>119</sup> ADVERTISERS, TRIPLELIFT, <https://triplelift.com/advertiser-solutions/>.

operators), TripleLift promises to “[u]nlock new revenue opportunities and drive incremental dollars effortlessly.”<sup>120</sup>

192. TripleLift specifically discusses its real-time bidding capabilities, noting it can provide “the most competitive price” for user inventory and “[d]ynamically adjust bids to reach the most relevant audiences”<sup>121</sup>:

**Figure 26:**



193. TripleLift also touts its integration with data brokers and other “data partners,” which it claims enables “advertisers to reach the right audience with precision. By leveraging first-party and contextual data, we deliver personalized and impactful ad experiences. Our data-driven targeting solutions ensure that your ads reach relevant users, boosting engagement and ROI”<sup>122</sup>:

**Figure 27:**



<sup>120</sup> PUBLISHERS, TRIPLELIFT, <https://triplelift.com/publisher-solutions/>.

<sup>121</sup> TRIPLELIFT SSP, <https://triplelift.com/triplelift-ssp/>.

<sup>122</sup> PARTNERS, TRIPLELIFT, <https://triplelift.com/partners/>.

194. “TripleLift Audiences,” meanwhile “packages audience segments spanning third-party and first-party data to deliver outcomes for advertisers today and in a cookieless future.”<sup>123</sup> Its use cases include “[a]dvertiser first-party data retargeting based on a known list of consumers.”<sup>124</sup>

195. By way of example, if a home-goods brand wants to use TripleLift to serve its ads, it can purchase TripleLift’s “Home Curated Deal” to reach “people who are investing their time and money close to home.”<sup>125</sup> By choosing this set of data, the home-goods brand will be able to target “audiences spending time on home improvement, home entertaining, outfitting their setups, browsing real estate, raising kids and adopting pets.”<sup>126</sup> This data set can be used for ads in the “Native, Display and Video” formats, “in placements known to deliver high viewability and high video completion rates.”<sup>127</sup> TripleLift ensures that these data sets “are refreshed on an on-going basis so that only the highest performing placements are included.”<sup>128</sup>

196. In short, by installing TripleLift’s Tracker on Website users’ browsers, Defendant and TripleLift can de-anonymize users by correlating their IP addresses, Device Metadata, and unique identifiers to profiles maintained data brokers, and sell those profiles to advertisers to enrich Defendant. TripleLift also benefits from this arrangement, as it collects additional information about users it can use in the future on behalf of other clients, and can continue to track now de-anonymized users across the Internet.

**D. Defendant Uses The OpenX Tracker For Targeted Advertising, Identity Resolution, And Data Monetization**

197. As noted above, OpenX is a registered Data Broker in California that claims to be “the world’s leading independent supply-side platform for audience, data, and identity targeting.”<sup>129</sup>

<sup>123</sup> SMART DATA & TARGERTING FOR ADVERTISERS, TRIPLELIFT, <https://web.archive.org/web/20240325054603/https://triplelift.com/products/audiences-advertisers/> (as accessed March 25, 2024).

<sup>124</sup> *Id.*

<sup>125</sup> HOME, TRIPLELIFT, <https://web.archive.org/web/20240405090112/https://triplelift.com/exchange-traded-deals/home/> (as accessed April 5, 2024).

<sup>126</sup> *Id.*

<sup>127</sup> *Id.*

<sup>128</sup> *Id.*

<sup>129</sup> *About Us*, OpenX, <https://www.openx.com/company/>



1           198. OpenX helps companies like Defendant “utilize their [first party] data, leverage [third  
2 party data], and package up audiences for marketers that will drive ad revenue.”<sup>130</sup> OpenX takes this  
3 data and uses it to “match [a company’s] audience against [OpenX’s] graph to put users in audience  
4 segments that [OpenX] mak[es] available to marketers.”<sup>131</sup>

5           199. OpenX can then use these individual profiles to provide marketers, such as Defendant,  
6 with curated packages that identify and target specific customers.<sup>132</sup>

7           200. OpenX splits this up into two different types of packages. The first are inventory  
8 packages that allows marketers to “[s]howcase [their] brand alongside brand-safe inventory across  
9 [OpenX’s] network of trusted publishers, reaching consumers *wherever* and *whenever* they engage  
10 with their favorite content.”<sup>133</sup>

11           201. The second are data driven packages that “[e]ngage customers with packages powered  
12 by data-driven curation, and drive performance on brand-safe inventory. [Allowing companies, like  
13 Defendant to e]ffortlessly choose from pre-built packages powered by audience, contextual,  
14 attention, or sustainability data and [OpenX’s] proprietary identity graph.”<sup>134</sup>

15           202. OpenX’s identity graph provides companies like Defendant, PubMatic, and TripleLift  
16 access to 800 million hashed emails, 200 million hashed phone numbers, over 200 million U.S. users  
17 instrumented for data and identity, 48 million CTV users instrumented for data and identity, over  
18 5,000 requests per user per month, and 3,000 data attributes available for targeting.<sup>135</sup>

19  
20 <sup>130</sup> *OpenAudience*, OPENX, <https://www.openx.com/why-openx/openaudience/> (last accessed Jan.  
21 27, 2025). First-party data is data that websites “collect directly from [their] customers,” while third-  
22 party data is data that is “acquire[d] from a data aggregator” that does “not collect data directly but  
23 obtain[s] it from other companies and compile[s] it into a single dataset.” WHAT IS THE DIFFERENCE  
24 BETWEEN FIRST-PARTY, SECOND-PARTY AND THIRD-PARTY DATA?, CUSTOMER DATA PLATFORM  
25 RESOURCE, <https://tinyurl.com/2htc6a8n>.

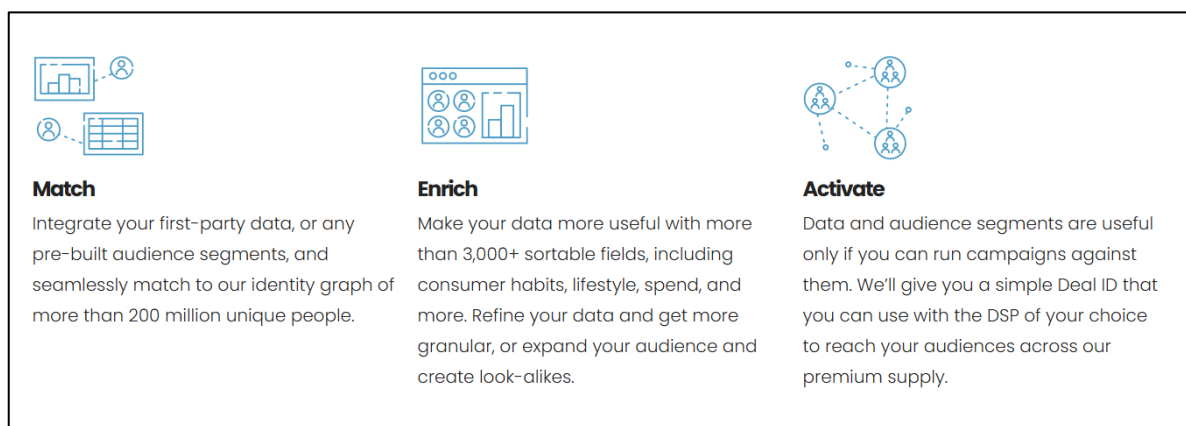
26 <sup>131</sup> *Data Activation*, OPENX, <https://www.openx.com/why-openx/openaudience/> (last accessed Feb.  
27 3, 2025).

28 <sup>132</sup> *Curated Packages*, OPENX, <https://www.openx.com/curated-packages/> (last accessed Feb. 4,  
2025).

<sup>133</sup> *Id.* (emphasis added).

<sup>134</sup> *Id.*

<sup>135</sup> *OpenAudience*, OPENX, <https://www.openx.com/why-openx/openaudience/>.

**Figure 28:**

203. By way of example, OpenX sells a “Health Insurance Data Driven Package” that targets consumers who have viewed advertisements from health insurance advertisers.<sup>136</sup> This helps companies target people who have indicated an interest in specific health insurance related content.

204. OpenX has previously been sued by the federal government for collecting personally identifiable information from users who specifically asked not to be tracked. *See United States of America v. OpenX Technologies, Inc.* Case No. 2:21-cv-09693-DMG-AGR (C.D. Cal.).<sup>137</sup>

205. To do all of this, OpenX needs to collect data that identifies a particular user. This is why OpenX collects IP addresses and Device Metadata: it allows OpenX to link one of Defendant’s Website users to any profile OpenX may have about that user, and OpenX can in turn provide that profile to interested advertisers for more targeted advertising. The IP address, Device Metadata, and unique user identifiers also allow OpenX to track a user’s Website activity over time (*i.e.*, through repeated Website visits) and to track that user on other websites. All of this helps Defendant further monetize its Website and maximize revenue by de-anonymizing users and procuring higher bids from advertisers in the process.

#### IV. PLAINTIFF’S EXPERIENCE

206. Plaintiff regularly visited the Websites on his desktop browser—as long ago as 2020 and as recently as February 2025—and has done so throughout the entirety of the class period.

<sup>136</sup> *Health Insurance Data Driven Package*, OPENX, <https://www.openx.com/curated-packages/health-insurance/>.

<sup>137</sup> ADVERTISING PLATFORM OPENX WILL PAY \$2 MILLION FOR COLLECTING PERSONAL INFORMATION FROM CHILDREN IN VIOLATION OF CHILDREN’S PRIVACY LAW, <https://tinyurl.com/yp3f2nm5>.

1           207. When Plaintiff visited the Website, the Website's code—as programmed by  
2 Defendant—caused the Trackers to be installed on Plaintiff's browser. *See* Figures 4, 6, 16-17 *supra*.

3           208. Through their respective Trackers, the Third Parties collected and recorded Plaintiff's  
4 IP address, Device Metadata, and set a cookie with a unique user ID that allowed the Third Parties  
5 to pervasively track Plaintiff across multiple Website sessions and even other websites, as well as  
6 de-anonymize Plaintiff by synchronizing his user profile amongst each other and with other entities.  
7 *See* Figures 7-12, 14-15, 18-20, 27-28, *supra*.

8           209. Defendant and the Third Parties used the information collected by the Trackers to:

- 9           (i) identity Plaintiff and either create a new profile of him in the  
10 Third Parties' databases or match Plaintiff to a pre-existing  
11 profile (either in the Third Parties' own databases or with  
12 another entity's profile);
- 13           (ii) sell Plaintiff's information to advertisers for hyper-targeted  
14 advertising based on the information collected by the Third  
15 Parties on the Website—including but not limited to  
16 Plaintiff's location information based on his IP address—  
17 and the information contained on any profiles of Plaintiff  
18 (which are linked to Plaintiff via the information collected  
19 by the Third Parties on the Website);
- 20           (iii) actually target Plaintiff with advertisements and serve  
21 advertisements on Plaintiff based on the information  
22 collected by the Third Parties—including but not limited to  
23 Plaintiff's location information based on his IP address—on  
24 the Website and the information contained on any profiles of  
25 Plaintiff (which are linked to Plaintiff via the information  
26 collected by the Third Parties on the Website); and
- 27           (iv) de-anonymize Plaintiff and generate revenue from the sale  
28 of Plaintiff's information—both what is collected on the  
Website by the Third Parties and the profiles this  
information is linked to—to advertisers, thus boosting  
Defendant's, advertisers', and the Third Parties' revenue and  
the value of the Third Parties' services.

23           210. Plaintiff did not provide his prior consent to Defendant to install or use the Trackers  
24 on his browser. Nor did Defendant obtain a court order before installing or using the Trackers.

25           211. Thus, Plaintiff has had his privacy invaded by Defendant's violations of CIPA  
26 § 638.51(a), and Defendant has likewise been unjustly enriched through the Third Parties'

1 surreptitious and unconsented-to collection of Plaintiff's data. Accordingly, Plaintiff has been  
2 injured by Defendant's violation of the CIPA.

3 **V. DEFENDANT IS SUBJECT TO JURISDICTION IN CALIFORNIA**

4 212. Defendant purposefully directed its conduct at California residents. Defendant took  
5 the intentional act of installing the Trackers (pen registers) on its users' browsers. This is so because  
6 Defendant programmed the code of its Website to install the Trackers, Defendant entered agreements  
7 with each of the Third Parties operating the Trackers for the provision of said Trackers, and  
8 Defendant used and profited off of the information surreptitiously and unlawfully collected by the  
9 Third Parties operating the Trackers.

10 213. Defendant expressly aimed its conduct at California. Defendant's Website relies  
11 mostly if not entirely on advertising revenue to provide its content. As noted above, the advertising  
12 on Defendant's Website is programmatic or based on "real-time bidding," meaning Defendant  
13 generates revenue by selling or sharing Website users' data with advertisers vis-à-vis the Third Party  
14 Trackers, and advertisers pay Defendant money through the Third Party Trackers to show specific  
15 Website users specific advertisements based on that data.

16 214. When a user accesses the Website, Defendant knows the location of that user because  
17 Defendant also receives the user's IP address, and a user's IP address correlates to their approximate  
18 location. Thus, if a California user accesses the Website, Defendant knows the user is accessing the  
19 Website from California, knows it is installing the Trackers on a California user's browser, knows  
20 that the data of California users is being shared with and sold to advertisers, and knows that it is  
21 profiting off the data of California users.

22 215. Crucially, Defendant knows a user is accessing its Website from California *before*  
23 Defendant installs the Third Party Trackers on the user's browser. Recall the technological order of  
24 operations. *See* Figure 1, *supra*. *First*, the user's browser communications with Defendant's  
25 Website. Through this transmission, Defendant learns the user's IP address, and therefore, the user's  
26 location. *Then*, Defendant's Website—as programmed by Defendant—responds with code or  
27  
28

1 instructions to install the Trackers on the user's browser. Thus, when Defendant installs the Trackers  
 2 on the user's browser, Defendant knows the location that the user is accessing the Website from.

3 216. Plaintiff was among the California residents whose information was sold to  
 4 advertisers, as caused by Defendant's knowing and intentional installation of the Trackers on  
 5 Plaintiff's browser. For example, as noted above, Defendant knew Plaintiff was in California when  
 6 it installed the ADNXS Tracker on his browser based on Plaintiff's IP address, and Microsoft also  
 7 collected Plaintiff's IP address through its Tracker, thus revealing Plaintiff's location to Microsoft.

8 217. The below screenshot shows that Defendant was using the ADNXS Tracker to fill a  
 9 "banner" advertising space.<sup>138</sup> The dimensions of the banner ad are listed as particular pixels—the  
 10 values for the "height" and "width" parameters. The "cpm" parameter shows the advertiser—  
 11 through the ADNXS Tracker that Defendant installed—was willing to pay approximately \$2.97 cost  
 12 per mille (CPM) to show Plaintiff an advertisement as a result of the information Microsoft provided  
 13 to the advertiser. CPM stands for "cost per mille," which "is a pricing model used in digital  
 14 advertising, where advertisers pay the publisher a fixed price for 1,000 impressions of their ad—  
 15 'mille' being Latin for 'thousand.' An impression is achieved when an ad loads on the page or app  
 16 and is viewed by the user."<sup>139</sup> Finally, the advertisement shows it was "served by Member 903 via  
 17 AppNexus," meaning one of the advertisers who partnered with Microsoft bid to serve the ad to  
 18 Plaintiff. As noted above, this would be one of many advertisers with whom Microsoft partnered  
 19 and shared Plaintiff's information and who placed a bid to show Plaintiff an advertisement.

20 //

21 //

22 //

23 //

24 //

25 <sup>138</sup> "Banners are the creative rectangular ads that are shown along the top, side, or bottom of a website  
 26 in hopes that it will drive traffic to the advertiser's proprietary site, generate awareness, and overall  
 27 brand consideration." WHAT IS BANNER ADVERTISING?, [https://advertising.amazon.com/library/  
 guides/banner-advertising](https://advertising.amazon.com/library/guides/banner-advertising).

28 <sup>139</sup> COST PER MILLE (CPM), <https://www.appsflyer.com/glossary/cpm/>

**Figure 29:**

```

"ads": [{
  "cpm": 2.970000,
  "cpm_publisher_currency": 2.970000,
  "publisher_currency_code": "$",
  "publisher_currency_codename": "USD",
  "content_source": "rtb",
  "ad_type": "banner",
  "buyer_member_id": 903,
  "creative_id": 593535178,
  "media_type_id": 1,
  "media_subtype_id": 1,
  "brand_category_id": 4,
  "brand_id": 1386531,
  "is_sov": false,
  "is_roadblock": false,
  "bidder_id": 52,
  "client_initiated_ad_counting": true,
  "is_managed": false,
  "no_consent": false,
  "rtb": {
    "banner": {
      "content": "<!-- Creative 593535178 served by Member 903 via AppNexus -->
      "width": 300,
      "height": 250
    }
  },

```

218. Given that iHeartMedia is the “#1 audio company in the United States,” has “4x [t]he reach of the largest ad-enabled streaming music audio service,” and has “[g]reater reach than any other media company in the U.S.,”<sup>140</sup> it is easy to see how even a purportedly low CPM can add up quickly when multiplied across millions of users and thousands of advertisements.

219. In sum, Defendant expressly aimed its conduct at California for at least the following reasons: (i) Defendant knew where Plaintiff’s and other Class Members’ browsers were accessing the Website from (California) “when it installed [the Trackers] on [Plaintiff’s and Class Members’] device[s]”; and (ii) Defendant knowingly profited from the disclosure and sale of Californians’ information through its installation and use of the Trackers. *See Briskin v. Shopify, Inc.*, 135 F.4th. 739, 746 (9th Cir. 2025).

<sup>140</sup> WE ARE IHEART MEDIA, <https://www.iheartmedia.com/>.

**CLASS ALLEGATIONS**

220. Pursuant to Fed. R. Civ. P. Rule 23(a) and 23(b)(3), Plaintiff seeks to represent a class defined as all California residents who accessed the Website in California and had their IP address, Device Metadata, and/or unique user identifiers collected by the Trackers (the “Website Class”).

221. Plaintiff also seeks to represent a subclass defined as all California residents who created an iHeart account, accessed the Website in California and had their IP address collected by the Trackers (the “Account Subclass”).

222. The Website Class and the Account Subclass shall be collectively referred to as the “Class.”

223. The following people are excluded from the Class: (i) any Judge presiding over this action and members of his or her family; (ii) Defendant, Defendant’s subsidiaries, parents, successors, predecessors, and any entity in which Defendant or their parents have a controlling interest (including current and former employees, officers, or directors); (iii) persons who properly execute and file a timely request for exclusion from the Class; (iv) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (v) Plaintiff’s counsel and Defendant’s counsel; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

224. **Numerosity:** The number of people within the Class is substantial and believed to amount to thousands, if not millions of persons. It is, therefore, impractical to join each member of the Class as a named plaintiff. Further, the size and relatively modest value of the claims of the individual members of the Class renders joinder impractical. Accordingly, utilization of the class action mechanism is the most economically feasible means of determining and adjudicating the merits of this litigation. Moreover, the Class is ascertainable and identifiable from Defendant’s records.

225. **Commonality and Predominance:** There are well-defined common questions of fact and law that exist as to all members of the Class and that predominate over any questions affecting only individual members of the Class. These common legal and factual questions, which do not vary



between members of the Class, and which may be determined without reference to the individual circumstances of any Class Member, include, but are not limited to, the following:

- (i) Whether Defendant violated CIPA § 638.51(a);
- (ii) Whether the Trackers are “pen registers” pursuant to Cal. Penal Code § 638.50(b);
- (iii) Whether Defendant sought or obtained prior consent—express or otherwise—from Plaintiff and the Class;
- (iv) Whether Defendant sought or obtained a court order for its use of the Trackers; and
- (v) Whether Plaintiff and members of the Class are entitled to actual and/or statutory damages for the aforementioned violations.

226. **Typicality:** The claims of the named Plaintiff are typical of the claims of the Class because the named Plaintiff, like all other members of the Class Members, visited the Website and had his IP address collected by the Trackers, which were installed and used by Defendant.

227. **Adequate Representation:** Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the Class Members he seeks to represent, he has retained competent counsel experienced in prosecuting class actions, and he intends to prosecute this action vigorously. The interests of members of the Class will be fairly and adequately protected by Plaintiff and his counsel.

228. **Superiority:** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of members of the Class. Each individual member of the Class may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant’s liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant’s liability. Class

1 treatment of the liability issues will ensure that all claims and claimants are before this Court for  
 2 consistent adjudication of the liability issues.

### 3 **CAUSES OF ACTION**

#### 4 **COUNT I**

#### 5 **Violation Of The California Invasion Of Privacy Act, 6 Cal. Penal Code § 638.51(a)**

7 229. Plaintiff repeats the allegations contained in the foregoing paragraphs as if fully set  
 8 forth herein.

9 230. Plaintiff brings this claim individually and on behalf of the members of the proposed  
 10 Class against Defendant.

11 231. CIPA § 638.51(a) proscribes any “person” from “install[ing] or us[ing] a pen register  
 12 or a trap and trace device without first obtaining a court order.”

13 232. A “pen register” is a “a device or process that records or decodes dialing, routing,  
 14 addressing, or signaling information transmitted by an instrument or facility from which a wire or  
 15 electronic communication is transmitted, but not the contents of a communication.” Cal. Penal Code  
 16 § 638.50(b).

17 233. The Trackers are “pen registers” because they are “device[s] or process[es]” that  
 18 “capture[d]” the “routing, addressing, or signaling information”—the IP address, Device Metadata,  
 19 and unique user IDs—from the electronic communications transmitted by Plaintiff’s and the Class’s  
 20 computers or smartphones (*i.e.*, “instruments”). Cal. Penal Code § 638.50(b).

21 234. Likewise, the Trackers are “pen registers” because they are “device[s] or process[es]”  
 22 that are being used to ascertain the identity of “visitors to Defendant’s [W]ebsite[s],” and are thus  
 23 capturing “addressing” information. *Heiting*, 2025 WL 736594, at \*3; *see also Greenley*, 684 F.  
 24 Supp. 3d at 1050 (“software that identifies consumers” is a pen register)).

25 235. At all relevant times, Defendant installed the Trackers—which are pen registers—on  
 26 Plaintiff’s and Class Members’ browsers, which allowed the Third Parties to collect Plaintiff’s and  
 27 Class Members’ IP addresses and Device Metadata. The Trackers also set a unique user identifier  
 28

1 on Plaintiff's and Class Members' browsers so the Third Parties could track Plaintiff and Class  
2 Members across multiple Website sessions and multiple websites.

3 236. Defendant and the Third Parties used the information collected by the Trackers to:

- 4 (i) identity Plaintiff and Class Members and either create new  
5 profiles of them in the Third Parties' databases or match  
6 Plaintiff and Class Members to pre-existing profiles (either  
7 in the Third Parties' own databases or with another entity's  
8 profile);
- 9 (ii) sell Plaintiff's and Class Members' information to  
10 advertisers for hyper-targeted advertising based on the  
11 information collected by the Third Parties on the Website—  
12 including but not limited to Plaintiff's and Class Members'  
13 location information based on their IP addresses—and the  
14 information contained on any profiles of Plaintiff and Class  
15 Members (which are linked to Plaintiff and Class Members  
16 via the information collected by the Third Parties on the  
17 Website);
- 18 (iii) actually target Plaintiff and Class Members with  
19 advertisements and serve advertisements on Plaintiff and  
20 Class Members based on the information collected by the  
21 Third Parties on the Website—including but not limited to  
22 Plaintiff's and Class Members' location information based  
23 on their IP addresses—and the information contained on any  
24 profiles of Plaintiff and Class Members (which are linked to  
25 Plaintiff and Class Members via the information collected by  
26 the Third Parties on the Website); and
- 27 (iv) (de-anonymize Plaintiff and Class Members and generate  
28 revenue from the sale of Plaintiff's and Class Members'  
information—both what is collected on the Website by the  
Third Parties and the profiles this information is linked to—  
to advertisers, thus boosting Defendant's, advertisers', and  
the Third Parties' revenue and the value of the Third Parties'  
services.

21 237. When Defendant installed and used the Trackers on Plaintiff's and Class Members'  
22 browsers—and when the Third Parties collected Plaintiff's and Class Members' information—  
23 Defendant knew that Plaintiff and Class Members were in California based on their IP addresses.  
24 Thus, Defendant harmed Plaintiff and Class Members knowing they were in California and  
25 unlawfully profited off Plaintiff's and Class Members' information knowing that information came  
26 from Californians.

238. The Trackers do not collect the content of Plaintiff's and the Class's electronic communications with the Website. *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1108 (9th Cir. 2014) ("IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication...") (cleaned up).

239. Plaintiff and Class Members did not provide their prior consent to Defendant's installation or use of the Trackers. Nor did Defendant obtain a court order to install or use the Trackers.

240. Pursuant to Cal. Penal Code § 637.2(a), Plaintiff and Class Members have been injured by Defendant's violations of CIPA § 638.51(a), and each seeks statutory damages of \$5,000 for each of Defendant's violations of CIPA § 638.51(a).

### **PRAYER FOR RELIEF**

WHEREFORE, Plaintiff, individually and on behalf of all others similarly situated, seeks judgment against Defendant, as follows:

- (a) For an order certifying the Class, naming Plaintiff as the representative of the Class, and naming Plaintiff's attorneys as Class Counsel to represent the Class;
- (b) For an order declaring that Defendant's conduct violates the CIPA;
- (c) For an order finding in favor of Plaintiff and the Class on all counts asserted herein;
- (d) For statutory damages of \$5,000 for each violation of CIPA § 638.51(a);
- (e) For pre- and post-judgment interest on all amounts awarded; and
- (f) For an order awarding and the Class their reasonable attorney's fees, expenses, and costs of suit.

### **JURY DEMAND**

Pursuant to Fed. R. Civ. 38(b), Plaintiff demands a trial by jury on all causes of action and issues so triable.

1 Dated: July 17, 2025

Respectfully submitted,

2 **BURSOR & FISHER, P.A.**

3 By: /s/ Philip L. Fraietta

4 Philip L. Fraietta (State Bar No. 354768)  
5 1330 Avenue of the Americas, 32nd Floor  
6 New York, NY 10019  
7 Telephone: (646) 837-7150  
8 Facsimile: (212) 989-9163  
9 E-mail: pfraietta@bursor.com

10 **BURSOR & FISHER, P.A.**

11 Joshua R. Wilner (State Bar No. 353949)  
12 1990 North California Blvd., 9th Floor  
13 Walnut Creek, CA 94596  
14 Telephone: (925) 300-4455  
15 Facsimile: (925) 407-2700  
16 E-mail: jwilner@bursor.com

17 **LABATON KELLER SUCHAROW LLP**

18 Michael P. Canty (*pro hac vice forthcoming*)  
19 Carol Villegas (*pro hac vice forthcoming*)  
20 Jonathan D. Waisnor (State Bar No. 345801)  
21 James M. Fee (*pro hac vice forthcoming*)  
22 Danielle Izzo (*pro hac vice forthcoming*)  
23 140 Broadway New York, NY 10005  
24 Telephone: 212-907-0700  
25 Fax: 212-818-0477

26 *Attorneys for Plaintiff*